Open Geospatial Consortium

Publication Date: 2016-01-25

Approval Date: 2015-09-17

Posted Date: 2015-07-21

Reference number of this document: OGC 15-051r3

Reference URL for this document: http://www.opengis.net/doc/PER/tb11-geo4niem-arch

Category: Public Engineering Report

Editor(s): Jeff Harrison

Testbed-11 OGC IP Engineering Report Geo4NIEM Architecture Design and Implementation Guidance and Fact Sheet

Warning

This document is not an OGC Standard. This document is an OGC Public Engineering Report created as a deliverable in an OGC Interoperability Initiative and is not an official position of the OGC membership. It is distributed for review and comment. This document 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 assess the potential for the National Information Exchange Model (NIEM) to be combined with security tags from Intelligence Community (IC) Data Encoding Specifications for information exchange. The assessment included reviewing Information Exchange Package Documentation (IEPD) populated with relevant content and IC security tags – and then deploying these instance documents on Open Geospatial Consortium (OGC) standards enabled Web Services for testing. The security tags included Information Security Marking Metadata (ISM) and Need-to-Know (NTK) Metadata for secure information exchange.

The assessment included reviewing example IEPDs and performing tests and demonstrations using OGC web services, such as Transactional Web Feature Services (WFS-T), Policy Enforcement Points (PEPs) and OGC Attribute Stores to process geographic feature with NIEM components and security tags. The Test and Demonstration included, but was not limited to, feature retrieval and transactions. Results were documented in this task to provide a preliminary architecture for Geo4NIEM in Testbed 11, and were described in technical detail in other OGC Testbed 11 Engineering Reports.

This document describes background considerations – and an overview of the services, data encodings and access control frameworks that compose the Geo4NIEM Testbed 11 architecture. This document must be reviewed in conjunction with the following Testbed 11 Geo4NIEM ERs:

- 15-048 Testbed11_Engineering_Report_NIEM-IC Data Encoding Specification Assessment and Recommendations
- 15-047 Testbed11_Engineering_Report NIEM-IC Feature Processing API using OGC Web Services
- 15-050 Testbed11_Engineering_Report Test and Demonstration Results for NIEM using IC Data Encoding Specifications

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

Testbed-11 OGC IP Engineering Report Geo4NIEM Architecture Design and Implementation Guidance and Fact Sheet

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 IC Data Encoding Specifications to be combined with NIEM for information exchange. The security tags included ISM, NTK and Trusted Data Format (TDF) to enable secure information exchange. The assessment included review of real world IEPDs, and this task performed Test and Demonstrations using the OGC Transactional Web Feature Service (WFS-T) standard, Policy Enforcement Points (PEPs) and OGC Attribute Stores to process GML feature representations leveraging NIEM components. Testing and demonstrations included, but were not limited to feature retrieval, insert, update and delete.

This task also identified potential change requests to the OGC WFS standard for handling security information in a federated role-based access control environment. These changes may help the NIEM/IC transform into more agile and customer-centric frameworks driven by collaborative partnerships. This transformation is vital to confronting the security challenges of the future.

This is especially important since geospatial interoperability efforts have matured to a point where broad acceptance is now dependent on the capacity to secure information exchanges. In fact, organizations that are considering participation in information exchanges must also consider how they can establish distributed security frameworks for role-based access control to resources. These requirements will continue to increase as data access transitions into data management with services like WFS-T where loosely affiliated parties collaborate on maintenance of shared situational awareness resources.

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 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 controls 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 and TDF metadata.

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[1]
- Incidents IEPD
- Resources IEPD

[1] For an example: https://mise.mda.gov/drupal/node/24

Recommendations to update these information exchanges were provided to reflect NIEM 3.0 architecture and included sample information 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-IC Feature Processing API using OGC Web Services ER.

1.2 Sponsoring and 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 the OGC Web Feature Service (WFS), the OGC) Filter Encoding Implementation Specification and the OWS Common Implementation Standard shall apply.

3.1 Abbreviated Terms

ABAC	Access Based Access Control
AIXM	Aeronautical Information Exchange Model
API	Application Programming Interface
ARH	Access Rights and Handling
DES	Data Encoding Specification
EDH	Enterprise Data Header
FES	Filter Encoding Specification
GML	Geography Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL/TLS
IC	Intelligence Community
IEPD	Information Exchange Package Documentation
IEP	Information Exchange Package
ISM	IC Security Markings
LDAP	Lightweight Directory Access Protocol
MDA	Maritime Domain Awareness
NIEM	National Information Exchange Model

NTK	Need to Know
OGC	Open Geospatial Consortium
OWS	OGC Web Services
PDP	Policy Decision Point
PEP	Policy Enforcement Points
PM-ISE	Program Manager for the Information Sharing Environment
RFC	Request For Comments
SAML	Security Assertion Markup Language
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

3.2 Used parts of other documents

This document uses significant parts of other OGC documents. This report refers to those documents by citing section designations, or copies some of those parts with small modifications.

4 Architecture Development

This section summarizes background considerations – and the services, data encodings and access control frameworks that compose the Geo4NIEM Testbed 11 architecture. These sections must be reviewed in conjunction with the following Testbed 11 Geo4NIEM ERs:

- 15-048 Testbed11_Engineering_Report: NIEM-IC Data Encoding Specification Assessment and Recommendations
- 15-047 Testbed11_Engineering_Report: NIEM-IC Feature Processing API using OGC Web Services
- 15-050 Testbed11_Engineering_Report: Test and Demonstration Results for NIEM using IC Data Encoding Specifications

4.1 Background Considerations

For Testbed 11 Geo4NIEM Thread, three service interfaces, encodings and information exchange frameworks were considered during architecture development:

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

4.1.1 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. 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.

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

This 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.

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

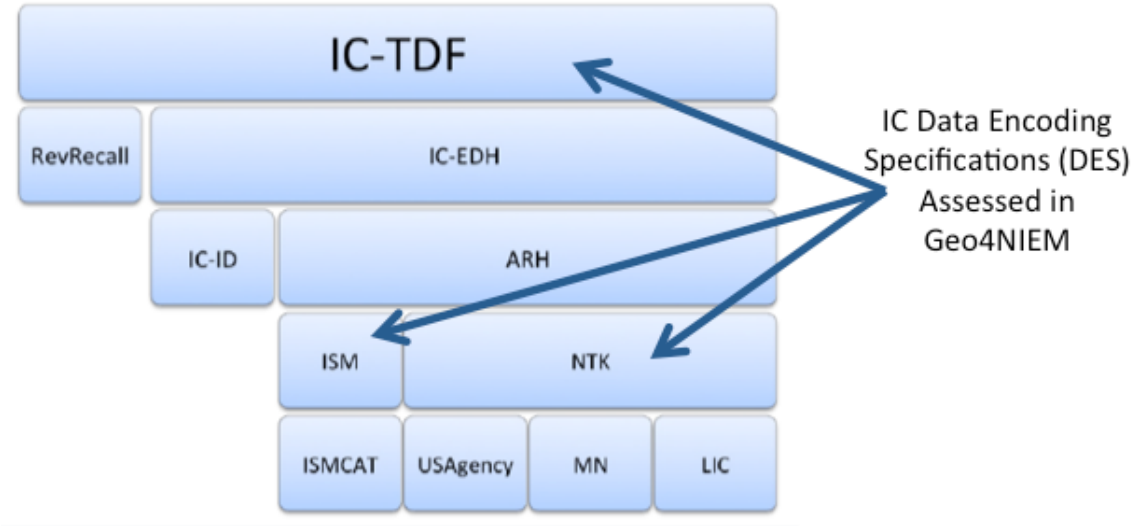
This XML Data Encoding Specification (DES) for Need-to-Know Metadata (NTK.XML) defines detailed implementation guidance for using XML to encode metadata necessary to facilitate automated systems making access control decisions. This DES defines the XML elements and attributes, associated structures and 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.

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

This 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[2]

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 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

[2] 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).

(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 have been successfully applied to a disaster management scenario.

4.1.5 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.

4.1.6 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.

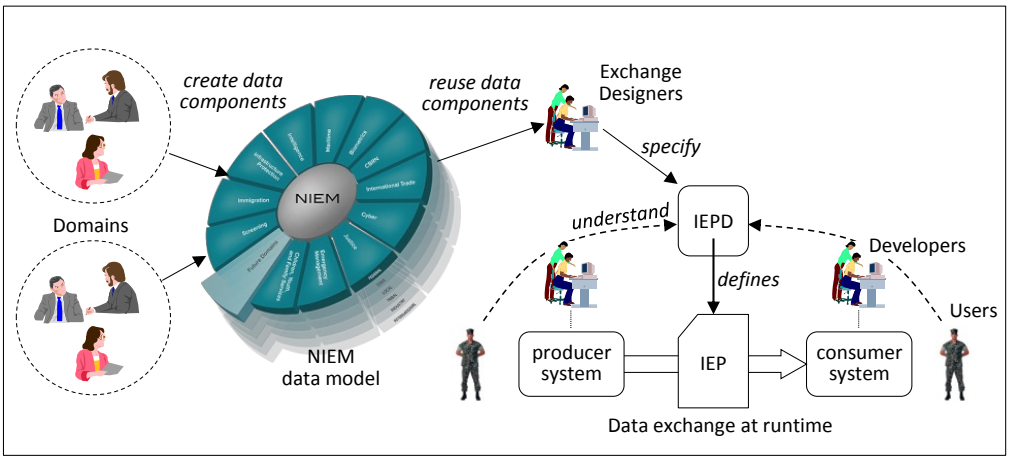


Figure 1 - The NIEM Process

4.1.7 OGC 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) and other formats from multiple Web Feature Services. The specification 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.

4.2 Geo4NIEM Testbed Architecture

The Testbed 11 Geo4NIEM Architecture has three main elements:

- NIEM-IC Data Encoding Specification
- NIEM-IC Feature Processing API
- Access Control Framework

The sections below must be reviewed in conjunction with the following Testbed 11 Geo4NIEM ERs:

- 15-048 Testbed11_Engineering_Report: NIEM-IC Data Encoding Specification Assessment and Recommendations
- 15-047 Testbed11_Engineering_Report: NIEM-IC Feature Processing API using OGC Web Services
- 15-050 Testbed11_Engineering_Report: Test and Demonstration Results for NIEM using IC Data Encoding Specifications

4.2.1 Data Encoding Specification

As a first step Trusted Data Objects (TDO) including ISM and NTK metadata in XML were added to the NIEM IEP documents along with GML feature geometries for testing. This process is summarized in the Figure below. The next step in the project was to serve the security-tagged NIEM/IC Data Encoding through an OGC Web Feature Service – Transactional (WFS-T).

A key consideration at this phase in the project was that the modular nature of the NIEM and IC security tags allows them to be combined in multiple ways to support the needs of information exchange. Accordingly, the encoding of the NIEM/IC Data Encoding on WFS needed to be flexible and allow for many different types IEP instance documents as input. For example, each Homeland Security domain may have many information exchanges, each with its own IEP documents for data exchange.

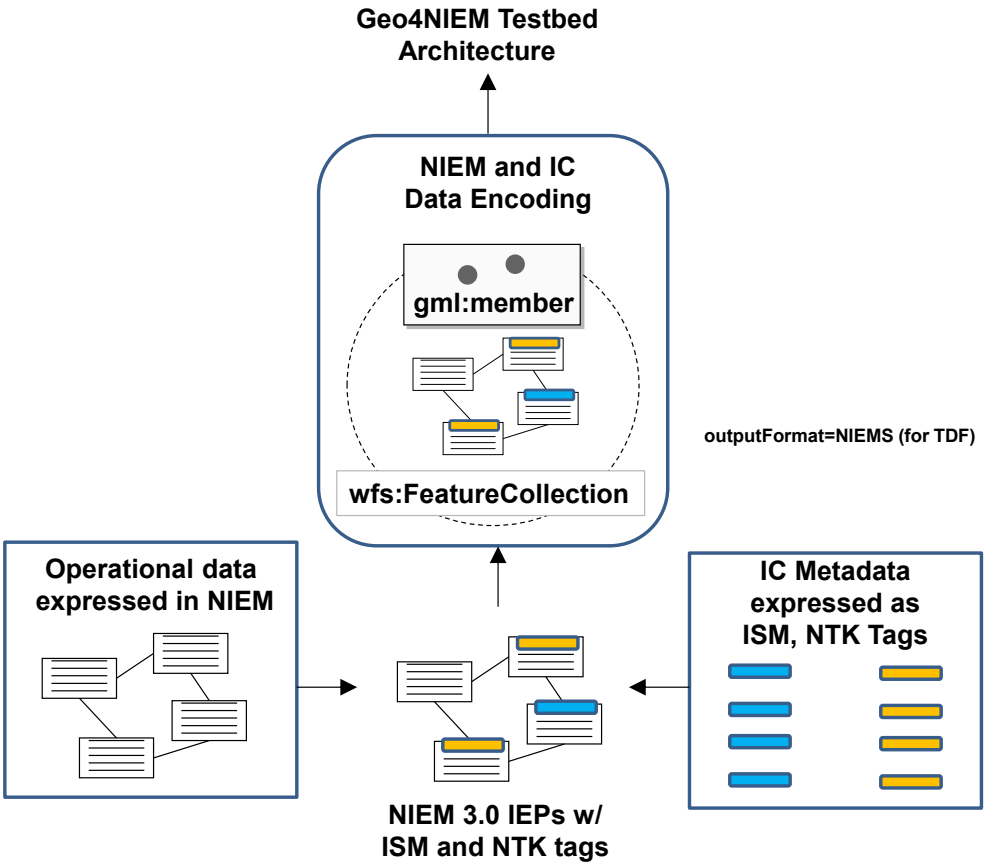


Figure 2 - Development of the NIEM-IC Data Encoding Specification

To support this 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, Notice of Arrival, Incident and Resource, were converted 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 other ERs as described above.

See 15-048 Testbed11_Engineering_Report: NIEM-IC Data Encoding Specification Assessment and Recommendations for additional detail.

4.2.2 Feature Processing API

In the Testbed 11: Geo4NIEM thread Participants assessed IC Security Markings and Need to Know tagging, and how to provide appropriate access control to NIEM IEPs served through a Web Feature Service.

The assessment was conducted by implementing prototype components that use a 'NIEM-IC Feature Processing API' 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, test results and demonstration are provided in a separate Engineering Report.

A representation of the key API points for NIEM-IC Feature Processing is provided below.

See 15-047 Testbed11_Engineering_Report: NIEM-IC Feature Processing API using OGC Web Services for additional details.

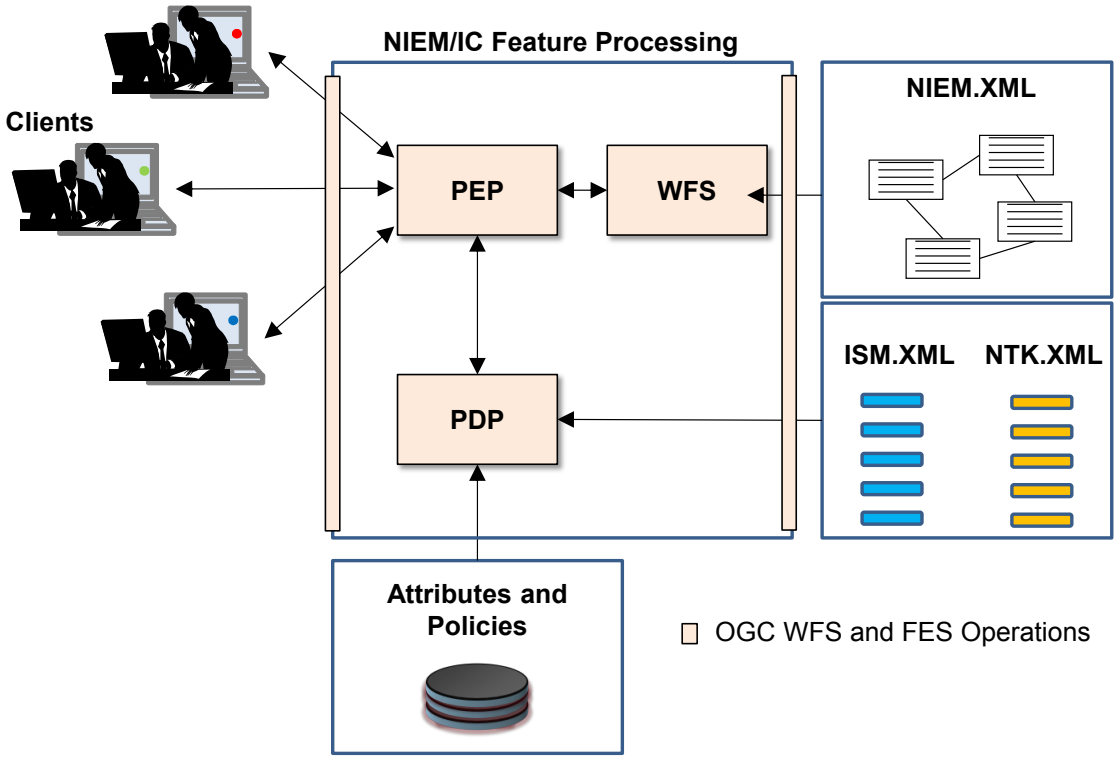


Figure 3 – Overview of the NIEM-IC Feature Processing API

4.2.3 Access Control Framework

A key consideration 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 NIEM/IC information exchange the 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.[3]

The access control portions of the Geo4NIEM architecture are shown in the representational flow diagram below.

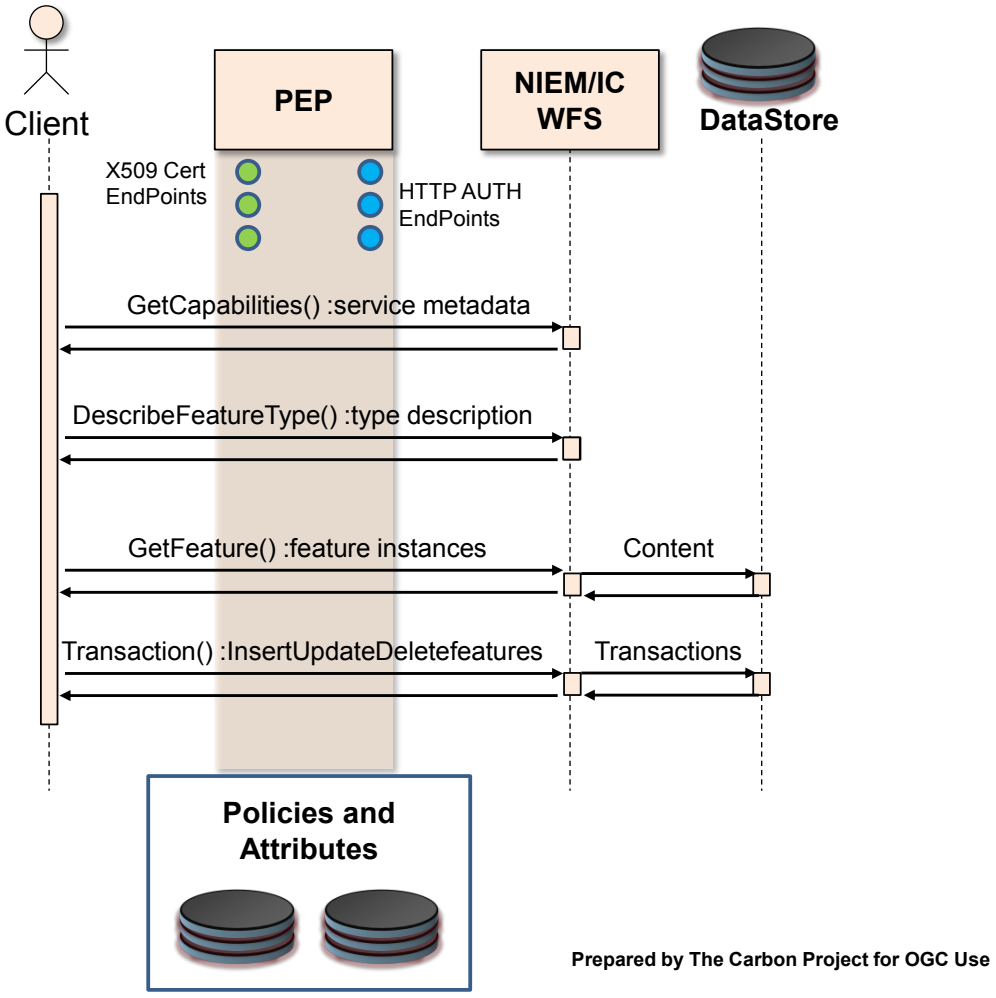


Figure 4 – Flow Diagram for Access Control (PEPs) in Geo4NIEM

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

See 15-050 Testbed11_Engineering_Report: Test and Demonstration Results for NIEM using IC Data Encoding Specifications for additional details.

5 Findings and Recommendations

The evidence obtained through the Testbed 11:Geo4NIEM testing and demonstration 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.

5.1 Combining NIEM, IC security, and 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 (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.

5.2 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.

5.2.1 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 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. 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.

Recommendation 3: Develop and test a Best Practice that defines more limited, but useful, subsets of NIEM 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.

5.2.2 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.

5.2.3 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.

5.3 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' NIEM-conformant 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

Geo4NIEM Testbed 11 Fact Sheet

This section provides a brief Fact Sheet[4] on Testbed 11 Geo4NIEM Thread.

Background

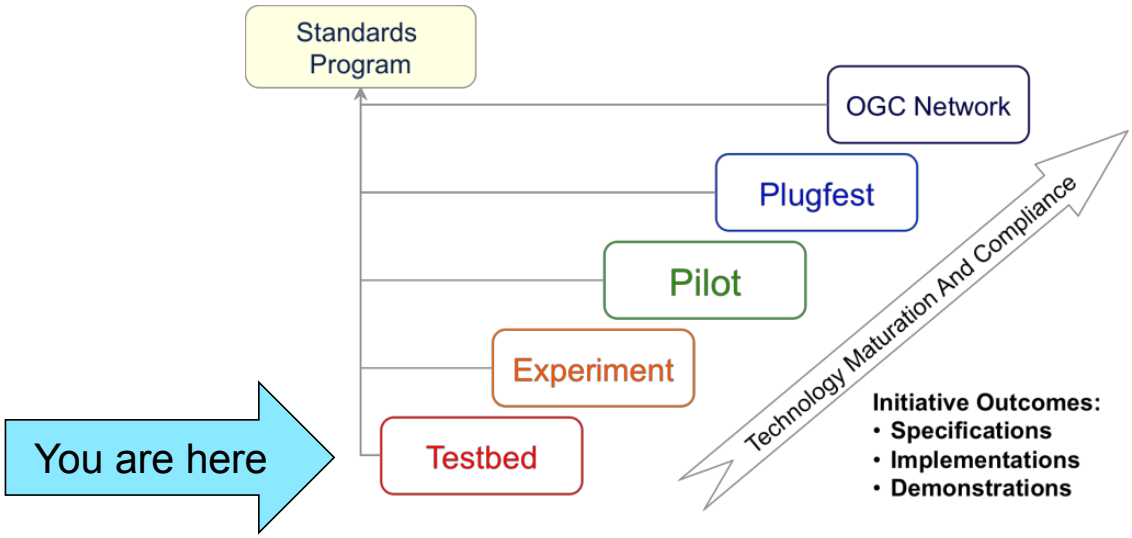
- **Geo4NIEM is an Open Geospatial Consortium (OGC) initiative examining how NIEM can works with OGC standards like GML**
- **The first round of Geo4NIEM concluded in 2013, demonstrating that**
  - NIEM information exchange packages (IEPs) can include GML-based data components
  - GML documents can include NIEM-based data components
- **The current round is part of OGC Testbed-11, ending now**
  - Engineering reports are nearly done; no major changes expected
- **Testbed results show that combining NIEM, IC Security, and OGC Web Services (OWS) is feasible**

OGC Testbed 11

- **Testbeds operate at the lowest level of maturity among the OGC interoperability initiatives**
  - Agree on a demonstration scenario
  - Participants connect existing products into a working demo
  - Demonstration experience informs the engineering reports

[4] Adapted from July 24 Geo4NIEM ESDP

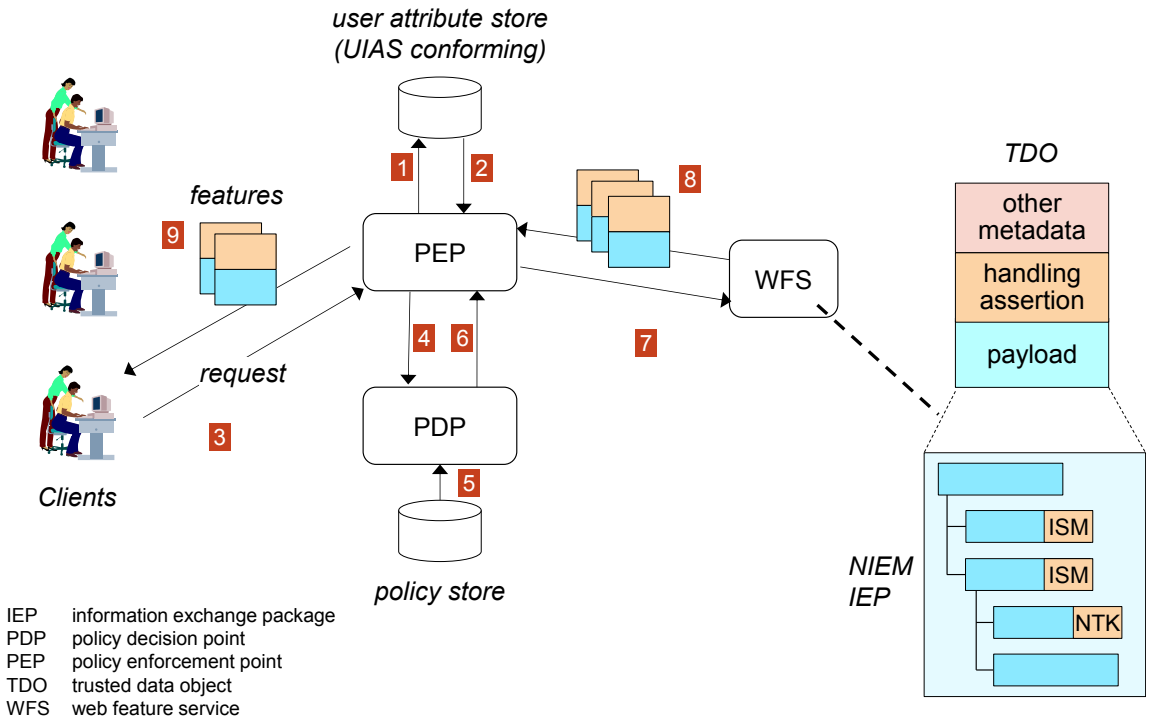
- ERs feed into the standards program and other processes



Geo4NIEM Tasks

1. **Assess support in NIEM for IC security specifications (ISM, NTK, TDF), and recommend a security architecture**
2. **Demonstrate secure information exchange using architecture from task 1**
3. **Assess NIEM and GML support for geospatial data exchange from NIEM-based client to GML-based client and back (round-trip); recommend a round-trip architecture**
4. **Demonstrate round-trip geospatial data exchange using the architecture from task 3**
5. **Demonstrate OGC Web Feature Service (WFS) on GML feature representations with embedded NIEM components**
6. **Analysis/study to reach consistent security approach across the OGC suite of service standards**

Architecture and Demo Sequence



Findings

- **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**
  - Access control engines can work with NIEM/IC data encoding, with or without a services framework
- **Implementing such a data exchange requires extra work, compared to a typical exchange of features that conform to the GML Simple Features profile**
  - This level of effort is not greater than encodings already in OGC, like AIXM, where a community of interest has defined a standard GML application schema for exchanging geographic data
- **Careful IEPD design can simplify the exchange implementation, reducing the technical overhead required to broadly implement secure information exchanges and emerging collaborative partnerships**

Recommendations for Future Work

- **Tools and best practices for exposing NIEM IEPs through the OGC Web Feature Service interface**
  - Includes making IEPD schemas available via WFS
- **Tools and best practices for expressing and enforcing access control policy in terms of IC security metadata**
- **Best practice for simplified IEPDs**
  - Location and time core elements in GML Simple Features profile
  - Model similar to Cursor-on-Target (CoT)

Conclusion

- **SUCCESS: NIEM 3.0, IC security, and OGC Web Services will work together**
- **Results have limited maturity**
  - Nothing resembling an operational environment in terms of message variety and load
  - Need follow-on work to examine more questions and collect more evidence before we can create best practices
- **Follow-on work may lead to**
  - Guidance on when to use NIEM, when to use GML, when and how to use both

Annex B

Geo4NIEM Demonstration Scenario and Use Cases

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.

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 5 - 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

Geo4NIEM Use Cases

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

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.

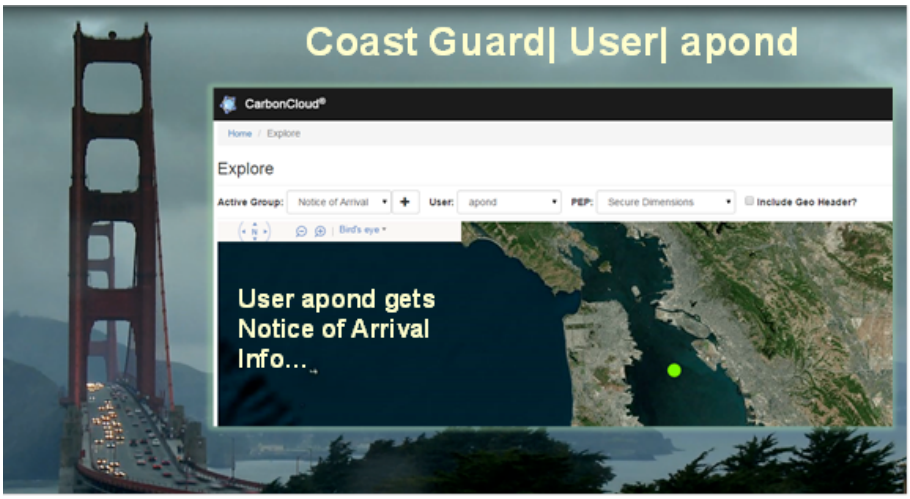
By including GML features into NIEM 3.0, and serving these messages via an OGC Web Feature Service, spatial and other filters can be invoked to receive a list of vessels that will be within the region (and with certain criteria). This allows the Port Authority to focus in on the ships that they really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

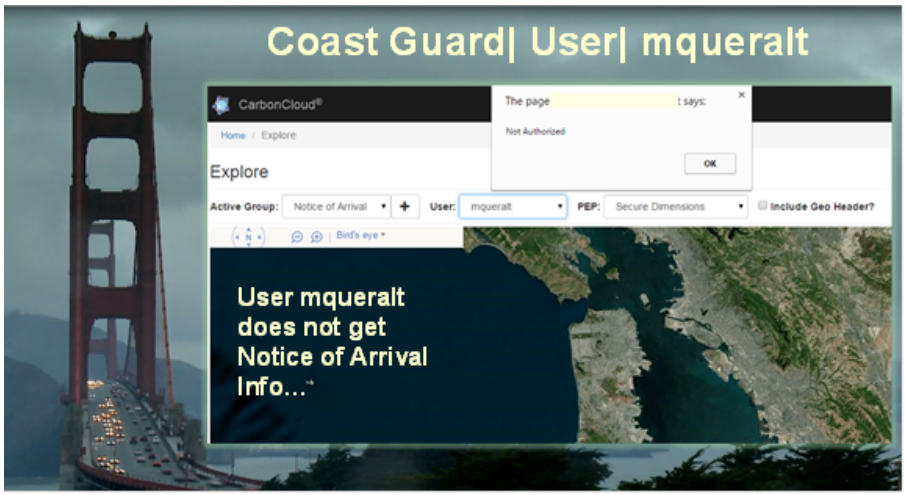
Some of the Notice of Arrival information is classified such as cargo type, some of this information might even be “top secret”, and the system cannot pass this information around to others, especially for cross-jurisdictional purposes, but they do need the minimum set of information for each feature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

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.





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.

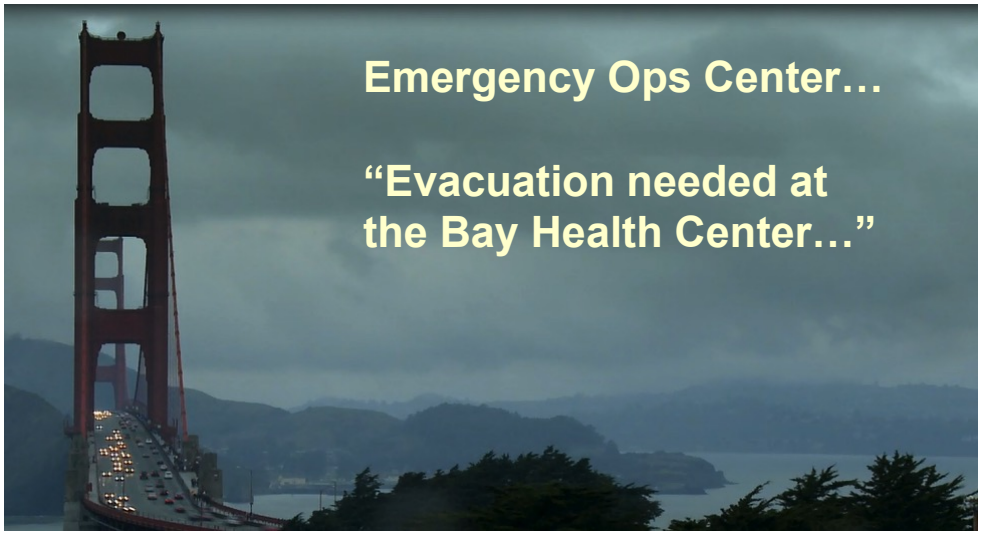
There are limited resources in the area due to all the responses that are in progress throughout the Bay Area. After the evacuation order has been given the Emergency Operations Center will need to notify others in the region of the incident, and request air resources to assist in the Air Ambulance evacuation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

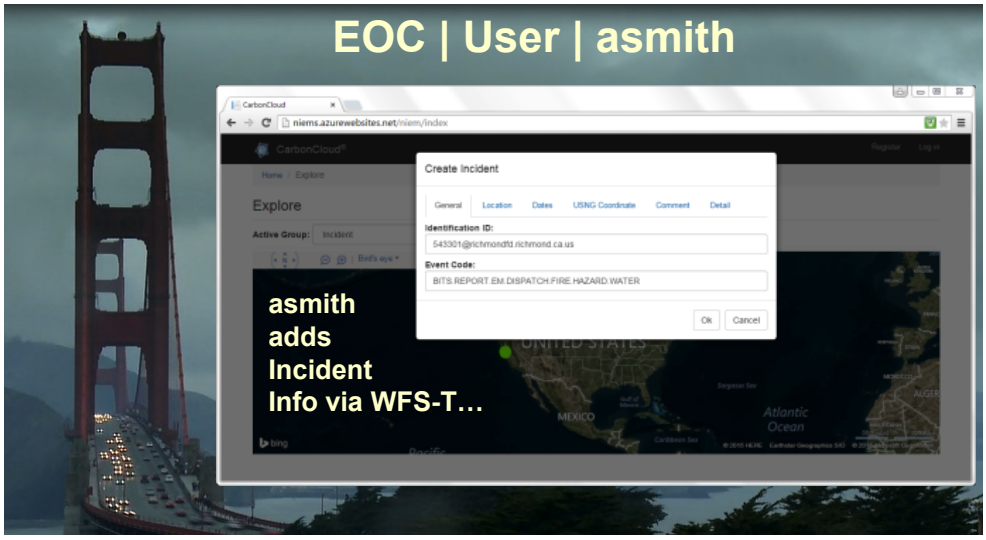
Knowing the geographical location of specific resources is now easier with the inclusion of OGC GML into the NIEM documents that allow for spatial filtering through the Web Feature Service.

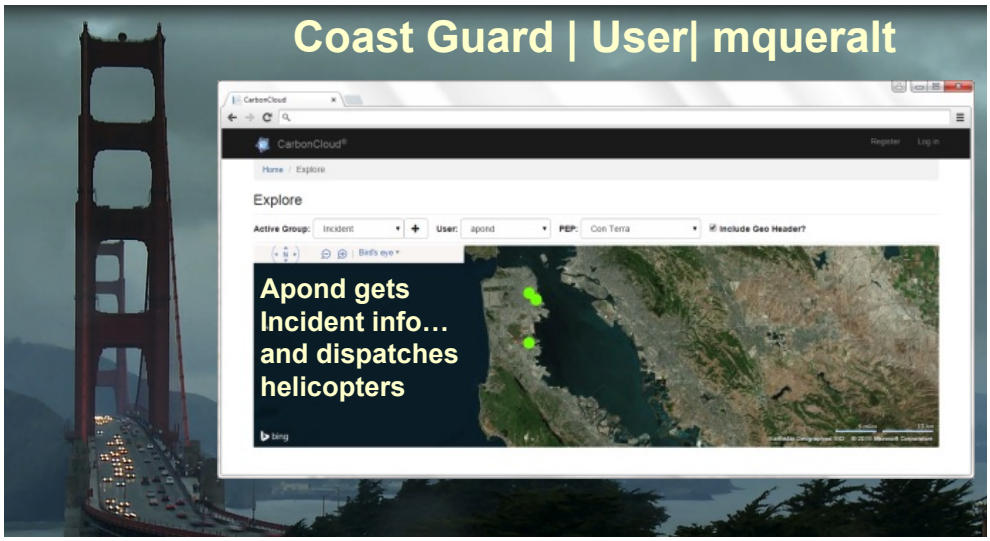
The back and forth nature of requesting resources and receiving responses regarding those resources stresses the requirements for the creation, search and retrieve, edit and update, and deletion of NIEM instance documents.

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.







Revision history

Date	Release	Editor	Primary clauses modified	Description
2013-05-14	02	J Harrison	All	Initial draft project deliverable.
2015-07-17	03	J Harrison	All	Abstract, Introduction, Graphics, and Findings updated based on TB11 test and demo activities
2015-09-19	04	J Harrison	All	Sponsor and Participant edits.
2015-10-12	05	J Harrison	All	Sponsor and Participant edits.
2015-9-14		C. Reed	Various	Final edits prior to publication.