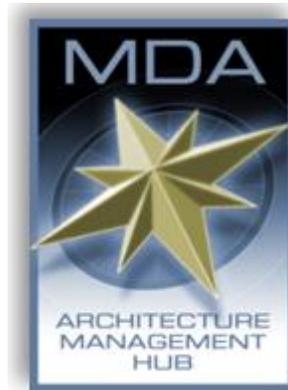


APPENDIX D - PUBLICATION INTERFACE SPECIFICATION



Maritime Information Sharing Environment (MISE)

Publication Interface Specification

Version 1.0

25 March 2013

1. Publication Overview

As discussed in the *National MDA Architecture*, information providers can choose between two integration approaches. In Figure 1, below, Information Provider System B chose to publish information to the Information Sharing Infrastructure (ISI) cache and delegate to the ISI the work of responding to access requests on behalf of users from information-consumer systems. This specification presents the details of the *Publication* interface used by a provider such as Figure 1's Provider B to keep the ISI cache up to date as a data set changes over time.

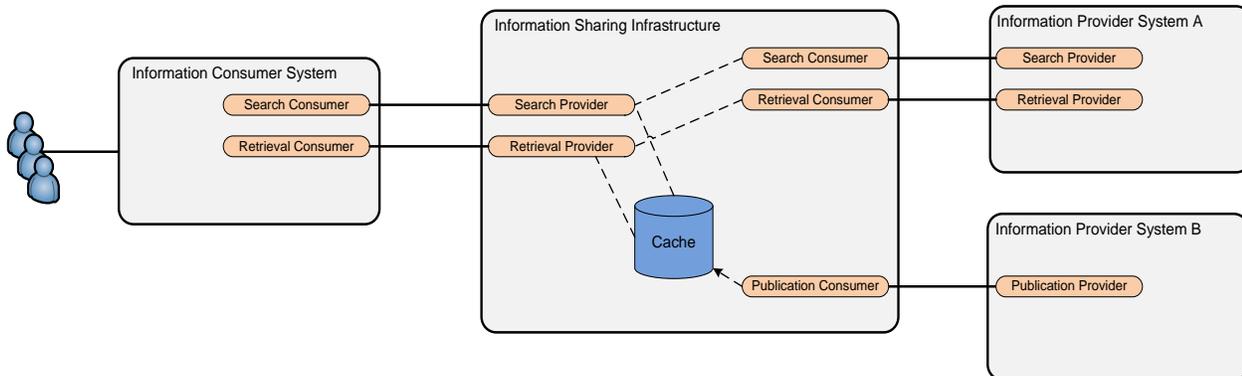


Figure 1 - Service Providers and Consumers

The publication interface follows the Representational State Transfer (REST) style. The ISI defines a URI endpoint for publication, and information-provider systems send HTTP requests and receive responses to URI paths beneath this URI endpoint. Details of these HTTP request and response messages are covered in Section 3.

All messages are authenticated and secured in the manner described in the *MISE Interface Security Specification*. For publication, the *Trusted System Authentication* portion of the interface security specification applies, but the *User Attribute Conveyance* portion does not apply since publication is not done on behalf of any individual user.

Each published data set must have an associated *Information Access Policy (IAP)*. This IAP information is carried in each record published to the ISI. For more information on the IAP, see the *MISE Attribute Specification* and the *National MDA Information Exchange Package Documents (IEPD)*. The IAP is carried via attributes in the XML documents published to the ISI.

2. Message Flow Patterns

This section describes the sequence of HTTP request/response messages that is expected to occur during normal operation. These processes help keep the ISI cache up to date.

2.1. INITIAL FULL PUBLICATION

Before publishing a data set, an information provider will work with MISE management to configure the trusted system and data set at the ISI. This includes creating an IAP for the data

set. Once these steps are complete, the information provider should do an initial full publication of the data set to the ISI, meaning all records that the information provider wishes to share should be sent to the ISI cache using the publication interface described herein.

The first step is to HTTP GET the version resource (see Section 3.1.1). If the version resource cannot be read, or if the version number is not one that the information provider is implemented to support, no further interaction with the interface should be taken.

After that, the information provider should HTTP PUT each individual shareable record (see Section 3.2.1). During this process, if the information provider fails to connect to the ISI, or if the ISI returns a status code indicating a server-side error (5xx), the information provider should periodically retry the PUT until it succeeds and contact the MISE helpdesk if errors persist.

If the information provider's back-end data store changes during the initial full publication, the provider system must track that and ensure that all shareable records have been successfully PUT to the ISI before the initial full publication process is considered complete.

Note that since the publication interface follows HTTP RESTful semantics, no harm is done if the information provider PUTs the same record more than once. The HTTP terminology for this characteristic is *idempotence*. Therefore, during any kind of error-recovery scenario, the provider is free to PUT the record if there is any question whether a previous PUT succeeded.

2.2. ONGOING UPDATING

After the initial full publication is complete, the information provider should update the ISI cache whenever any changes occur to the set of shareable records.

As with initial full publication, the information provider should periodically HTTP GET the version resource to confirm that the version of the publication interface is compatible. This does not necessarily need to be done before each record update, but it should be checked frequently—at least daily. The version resource is defined to support If-Modified-Since to make the check highly efficient.

Whenever any shared record is added or changed in the provider's back-end data store, the full record should be sent to the ISI using HTTP PUT (see Section 3.2.1). Whenever any shared record is deleted from the provider's back-end data store, the provider should use HTTP DELETE (see Section 3.2.2) to delete the record from the ISI cache. If the information provider fails to connect to the ISI, or if the ISI returns a status code indicating a server-side error (5xx), the information provider should periodically retry the PUT or DELETE until it succeeds and contact the MISE helpdesk if errors persist. Note that the HTTP DELETE method is also idempotent, so the provider is free to DELETE the record if there is any question whether a previous DELETE succeeded.

3. Resource Reference

This section presents details of resources defined as part of the publication interface and aspects of HTTP protocol usage that are important to interoperability.

All URIs are defined relative to *<BaseURI>*, which represents the HTTP endpoint of the publication interface at the ISI. The physical URI will be provided when the trusted system is

integrated with the ISI. For example only, this specification uses <https://isi.gov/publish> as the base URI.

3.1. METADATA

3.1.1. INTERFACE VERSION

The version of the MISE publication interface described in this document is 1.0. Before interacting further, an information provider should GET the version resource to confirm that the ISI interface version matches what is expected by the information provider implementation.

Table 1 presents details of the HTTP GET request an information provider uses to retrieve the version resource and the possible responses, which may be received back from the ISI.

URI	<BaseURI>/version	Example: https://isi.gov/publish/version
Method	GET	
Request Headers	Authorization	As described in the <i>MISE Interface Security Specification</i> .
	If-Modified-Since	Information provider system may send this header if it has previously read and cached this resource.
Request Content Type		Empty
Status Codes	200 (OK)	Successful. Response content as described below.
	304 (Not Modified)	The version resource has not been modified since the time specified in the If-Modified-Since request header.
	401 (Unauthorized)	No Authorization header or userid/password does not match any trusted system.
Response Headers	Last-Modified	
Response Content Type	application/xml; charset=UTF-8	Response content only returned if status code is 200.
Response Content	<pre><?xml version="1.0" encoding="UTF-8"?> <MISEInterface> <Name>Publication</Name> <MajorVersion>1</MajorVersion> <MinorVersion>0</MinorVersion> </MISEInterface></pre>	

Table 1 – Version Resources

3.2. RECORD

The record resource represents an individual record as stored in the ISI cache.

The URI for an individual record is <BaseURI>/<IEPDName>/<RecordID>, where:

- *<IEPDName>* matches one of the three currently defined national information products (noa, ian, pos).
- *<RecordID>* is assigned by the information provider. It is unique to an individual record within the scope of the provider’s data set.

For example, a full record URI may be similar to <https://isi.gov/publish/noa/12345>.

Before a record URI may be accessed, the ISI must be configured to accept a particular IEPD type from the provider. As discussed in the *MISE Interface Security Specification*, all HTTP requests to the ISI are authenticated, so the ISI knows which provider data set the record URI refers to—even though that information is not encoded within the URI. Records associated with a particular information provider cannot be accessed in any way through the publication interface by any other information provider.

3.2.1. ADD OR UPDATE A RECORD

Table 2 presents details of the HTTP PUT request an information provider uses to add or update a record and the possible responses, which may be received back from the ISI.

URI	<i><BaseURI>/<IEPDName>/<RecordID></i>	Example: https://isi.gov/publish/noa/12345
Method	PUT	
Request Headers	Authorization	As described in the <i>MISE Interface Security Specification</i> .
Request Content Type	application/xml; charset=UTF-8	
Request Content	NIEM-M representation of record.	Must validate against the schema for <i>IEPDName</i> but need not include a <i>schemaLocation</i> attribute. The XML declaration should specify UTF-8 encoding.
Status Codes	201 (Created)	Record did not previously exist at ISI and was successfully added.
	204 (No Content)	Record previously existed at ISI and was successfully updated.
	400 (Bad Request)	Request content did not validate against the schema for <i>IEPDName</i> .
	401 (Unauthorized)	No Authorization header, or <i>userid/password</i> does not match any trusted system.
	403 (Forbidden)	Authenticated information provider is not configured at ISI for publication of this IEPD.
Response Headers	Location	Only sent with status code 201. Matches record URI of request.

Response Content Type	Empty
-----------------------	-------

Table 2 – Adding or Updating Resources

3.2.2. DELETE A RECORD

Table 3 presents details of the HTTP DELETE request an information provider uses to delete a record and the possible responses, which may be received back from the ISI.

URI	<BaseURI>/<IEPDName>/<RecordID>	Example: https://isi.gov/publish/nea/12345
Method	DELETE	
Request Headers	Authorization	As described in the <i>MISE Interface Security Specification</i> .
Request Content Type	Empty	
Status Codes	204 (No Content)	Record was successfully deleted if it existed.
	401 (Unauthorized)	No Authorization header, or userid/password does not match any trusted system.
	403 (Forbidden)	Authenticated information provider is not configured at ISI for publication of this IEPD.
Response Content Type	Empty	

Table 3 – Deleting Records

3.2.3. PUBLISHING WITH A DATA SCOPE

For specific events and situations, the ISI provides the means for a data provider to specify a different level of data access. For instance, a data provider might allow temporary access to vessel position data for a wider range of data consumers during a hurricane. To publish data in a specific scope, the data provider must provide the **Scope** and **DataAttribute** parameters. A new record can be published with scope, or an existing record can be updated with a new scope.

URI	<BaseURI>/<IEPDName>/<RecordID>?<Scope=XXX>&<DataAttribute=YYYl>&<Releasable=B>&<Nation=NNN,MM M	Example: https://isi.gov/publish/nea/12345?Scope=HurricaneKatrina&DataAttribute=COI&Releasable=F&Nation=USA
Scope	String defining the scope in which this record has modified data access. These are defined by the MISE Board for specific events	HurricaneKatrina
DataAttribute	This is the modified data access attribute for that scope, as defined in the <i>MISE Attribute Specification</i> .	COI
Releasable	Optional. Boolean. Indicates whether the data is	T or F

	releasable within the scope.	
Nation	Optional. Comma-separated list of ISO 3-letter country codes. Indicates which nations to which the data can be provide in this scope.	USA,CAN
Method	PUT	
Request Headers	Authorization	As described in the <i>MISE Interface Security Specification</i> .
Request Content Type	application/xml; charset=UTF-8	
Request Content	NIEM-M representation of record.	Must validate against the schema for <i>IEPDName</i> but need not include a <i>schemaLocation</i> attribute. The XML declaration should specify UTF-8 encoding.
Status Codes	201 (Created)	Record did not previously exist at ISI and was successfully added.
	204 (No Content)	Record previously existed at ISI and was successfully updated.
	400 (Bad Request)	Request content did not validate against the schema for <i>IEPDName</i> .
	401 (Unauthorized)	No Authorization header, or userid/password does not match any trusted system.
	403 (Forbidden)	Authenticated information provider is not configured at ISI for publication of this IEPD.
Response Headers	Location	Only sent with status code 201. Matches record URI of request.
Response Content Type	Empty	

Table 4 – Adding or Updating a Record with Data Scope

3.2.4. RECORD EXPIRATION

Records in the ISI cache will always be considered expired and be deleted after 30 days in the cache. Data providers can exercise more precise control over their records via the following means:

1. The DELETE interface described in 3.2.2, above.

1. Each IEPD includes the DocumentExpirationDate element. When set to a value less than 30 days, the record will be expired and deleted from the cache when that date is reached. If set to more than 30 days, it will be ignored and the record is deleted at 30 days.

VERSION 3.0
RELEASE 1
FEBRUARY 2015