Open GIS Consortium Inc.

Date: 2003-06-02

Reference number of this OpenGIS© Project Document: **OGC 03-063r1**

Version: 0.5.0

Category: OpenGIS© OGC Interoperability Program Report -Viewpoint Specification

Editors: Joshua Lieberman (Syncline Inc.)

Critical Infrastructure Collaborative Environment Architecture:

Computational Viewpoint

03-063r1

Warning

This document is not an OGC Standard or Specification. This document presents a discussion of technology issues considered in an Interoperability Initiative of the OGC Interoperability Program. The content of this document is presented to create discussion in the geospatial information industry on this topic; the content of this document is not to be considered an adopted specification of any kind. This document does not represent the official position of the OGC nor of the OGC Technical Committee. It is subject to change without notice and may not be referred to as an OGC Standard or Specification. However, the discussions in this document could very well lead to the definition of an OGC Implementation Specification.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type:	OpenGIS© Draft Interoperability Program Report -Viewpoint Specification
Document subtype:	OGC Critical Infrastructure Protection Initiative (CIPI)
Document stage:	Draft
Document language:	English

Contents

i. Preface

The Open GIS Consortium (OGC) is an international industry consortium of more than 250 companies, government agencies, and universities participating in a consensus process to develop publicly available geo-processing specifications. This Draft Interoperability Program Report (DIPR) is a product of the OGC Critical Infrastructure Protection Initiative (CIPI), the objective of which is to provide a vendor-neutral interoperable framework that enables collaborating communities to rapidly and collaboratively publish, discover, integrate and use geospatial information concerned with the protection of critical infrastructure systems in a range of sectors. Specifically, this document specifies a Computational Architecture viewpoint for a Critical Infrastructure Collaborative Environment (CICE).

The OGC Critical Infrastructure Protection Initiative is part of the OGC's Interoperability Program: a global, collaborative, hands-on engineering and testing program designed to deliver prototype technologies and proven candidate specifications into the OGC's Specification Development Program. In OGC Interoperability Initiatives, international teams of technology providers work together to solve specific geo-processing interoperability problems posed by Initiative sponsors.

ii. Document Contributor Contact Points

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

CONTACT	COMPANY	ADDRESS	PHONE/FAX	EMAIL
Joshua Lieberman	Syncline Inc.	373 Washington Street, Boston, MA 02108	Tel: 617-603-2209 Fax: 617-986-1001	jlieberman@syncline.com
Henry Han	York University	4700 Keele Street, Toronto, M3J 2P3	Tel: 416-736-2100 x 33482	hhan@yorku.ca
Charles Heazel	OGC	483 B Carlisle Dr. Herndon, VA 20170	703.380.7433	cheazel@opengis.org
John Davidson	Image Matters	105 South King St Leesburg, VA 20175	703-669-5510	johnd@imagemattersllc.com

iii. Revision history

Date	Release	Description
2003-01-17	0.1.0	▪ Template populated with the preliminary table of contents;
2003-03-09	0.2.0	▪ Updated TOC
2003-03-13	0.3.0	▪ Added content from RFQ Annex B
2003-05-19	0.4.0	▪ Revised with new document number
2003-06-01	0.5.0	▪ Added Section 2.4 CICE Services and Interactions; other misc. editorial changes
		▪
		▪
		▪
		▪

CIPI Computational Viewpoint Specification

1 Introduction

ISO RM-ODP (ISO/IEC 10746) is the architectural framework adopted by the OGC for specifying its reference architectures. The four main parts of the standard define viewpoints on open distributed processing (ODP) systems. This specification addresses the computational viewpoint for systems dedicated to the protection of critical infrastructure components; this viewpoint is concerned with the kinds of computations handled by the system and modes of access for those computations.

1.1 Scope

This draft Interoperability Program Report (DIPR) specifies the information viewpoint for the Critical Infrastructure Collaborative Environment (CICE). This open, distributed processing environment crosses organizational boundaries and includes a variety of components deployed within multiple communities. The CICE leverages OGC Web Services to enable:

- the publication of the availability of critical infrastructure services and data;
- the registration and categorization of published service and data providers; and
- the discovery and use of needed critical infrastructure services and data

Critical infrastructure is a very broad term that encompasses many large-scale systems in a range of sectors: energy, telecommunications, transportation, public health services, and more. Safeguarding such systems involves a welter of political, economic, and legal issues that will not be raised here. Rather, the CICE is more about the creation and maintenance of a *common information space* to support sense-making and decision-making activities on the part of incident response teams.

1.2 Conformance

Assessing conformance requires consistency across the various viewpoints (i.e. clear mappings of concepts) and across the models they define. In general, the set of viewpoint specifications should not make mutually contradictory statements. Furthermore, each specification should include correspondence statements that relate it to other viewpoints.

1.3 Normative references

The following normative documents contain provisions that, through reference in this text, constitute provisions of this Interoperability Program Report. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this document are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies.

ISO/IEC 10746-2:1996, *Information Technology – Open Distributed Processing –Reference Model: Foundations*.

ISO/IEC 10746-3:1996, *Information Technology – Open Distributed Processing –Reference Model: Architecture.*

1.4 Terms and definitions

For the purposes of this Interoperability Program Report, the terms and definitions given in ISO 10746-2 and ISO 10746-3 apply. For convenience, some of these terms are repeated below.

1.5 Policy

A set of obligation, prohibition, or permission rules that either constrain or enable actions, as related to a purpose. [ISO 10746-2]

1.6 Conventions

1.6.1 Symbols and abbreviated terms

The following symbols and abbreviated terms are used in this document.

API	Application Programming Interface
OGC	OpenGIS Consortium
XML	Extensible Markup Language

1.6.2 Requirement levels

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

2 CICE Computational Viewpoint

The Critical Infrastructure Collaborative Environment (CICE) Architecture is based on the need to enhance the ability of organizations and individuals to use geospatial processing technologies in an open distributed processing environment to address issues associated with assuring the continuity, viability and protection of a nation's critical infrastructure.

This open distributed architecture for CICE is described from four non-overlapping viewpoints: Enterprise, Information, Computational, and Engineering. This document focuses on the Computational perspective. The computational viewpoint is concerned with how geospatial software services plug into broader interoperability infrastructure to use and extend diverse, loosely coupled sources of data and services in support of Critical Infrastructure Protection. Accordingly, this computation first defines the core concepts of services, interfaces and operations (and the relationships amongst these concepts) for Critical Infrastructure Protection, and then describes the Publish/Find/Bind pattern that represents the interactions among OGC services. The computational viewpoint of the CICE also includes service classification and a description of the provided Service Framework.

2.1 Service-oriented architecture

A *service* is a collection of operations, accessible through an interface, which allows a user to evoke a behavior of value to the user. Typically, a service can be invoked using standardized protocols by a client from across a network independently of the platform, language and object model on which it was deployed.

In the CICE, there are three essential roles:

- Service Provider - publishes services to a broker (registry) and delivers services to service requestors.
- Service Requestor - performs discovery operations on the service broker to find the service providers it needs and then accesses service providers for provision of the desired service.
- Service Registry - helps service providers and service requestors to find each other by acting as a clearinghouse of services and content that can be used to discover and broker.

Figure 1 depicts three basic and one optional operation that occur between requestor, provider and registry services. Note that many readers should also recognize Figure 1 as most of the recent web services white papers and product literature include similar diagrams that map onto it directly. In many cases 'export', 'import', and 'service interaction' substitute for 'publish', 'find' and 'bind', respectively.

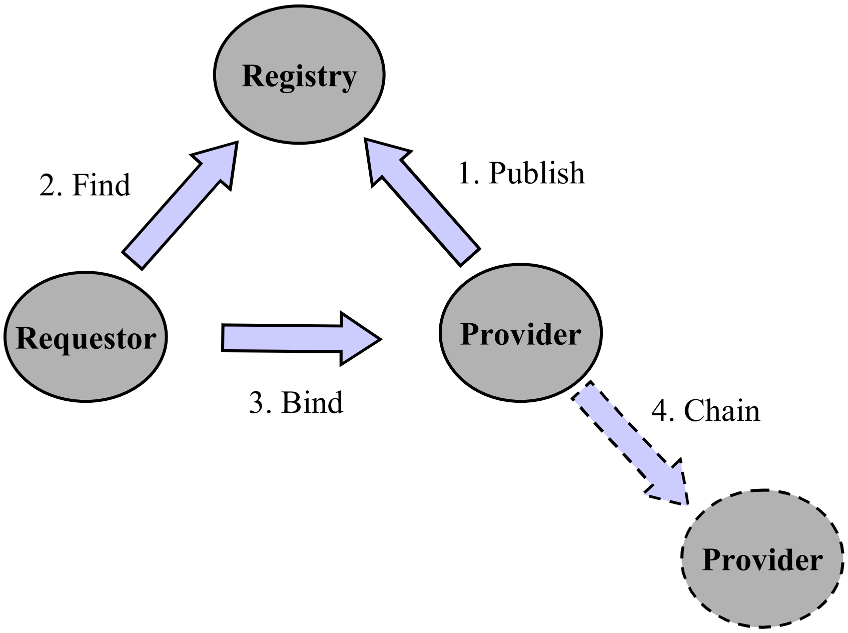

Figure 1. Service Types and Operations of the IPSM

As shown, there are three essential kinds of operations performed by services:

> Publish - The publish (and unpublish) operation is used to advertise (or remove) data and services to a broker (e.g., a registry, catalog or clearinghouse). A service provider contacts the service broker to publish or unpublish a service. A service provider typically publishes metadata to the registry describing, for example, its capabilities and network address.
>
> Find - Service requestors and service brokers collaborate to perform the find operation. Service requestors describe the kinds of services they're looking for to the broker and the broker delivers the results that match the request. Service requestors typically use metadata published to the registry to find service providers of interest.
>
> Bind - The bind operation takes place between a service requestor and a service provider. The two parties negotiate as appropriate so the requestor can access and invoke services of the provider. A service requestor typically uses service metadata provided by the registry to bind to a service provider.

And one optional operation:

> Chain - The chain operation binds a sequence of services where, for each adjacent pair of services, occurrence of the first action is necessary for the occurrence of the second action.

The CICE distinguishes between description of service type and service implementation. This allows service requesters to bind to a specific implementation of a service provider at development time, at deployment time, or dynamically at runtime. The CICE uses service descriptions (i.e., metadata about services) to support Publish, Find, Bind and Chain operations. Service metadata plays three distinct roles:

- Metadata specifies the characteristics of a service provider. Service brokers use these characteristics to categorize service providers to support the find operation. The classification of services can be based on one or more hierarchical service taxonomies. Service requesters use these characteristics to match a service provider to their requirements.
- Metadata specifies non-functional characteristics such as security, transactional requirements, cost of using the service provider, and others. Non-functional characteristics may be used to help a service requester find a service provider.

Metadata describes the interfaces used to access the service. The interface description includes its signature, allowed operations, data typing, and the access protocols. Service requesters use this information to bind to the service provider and invoke its services using the published interfaces.

2.2 CICE Services Framework

CICE Services are implementations of services that conform to OpenGIS Implementation Specifications. Compliant applications, called OpenGIS Applications, can then "plug into" the framework to join the operational environment.

By building applications to common interfaces, each application can be built without a-priori or run-time dependencies on other applications or services. Applications and services can be added, modified, or replaced without impacting other applications. In addition, operational workflows can be changed on-the-fly, allowing rapid response to time-critical situations. This loosely coupled, standards-based approach to development results in very agile systems—systems that can be flexibly adapted to changing requirements and technologies

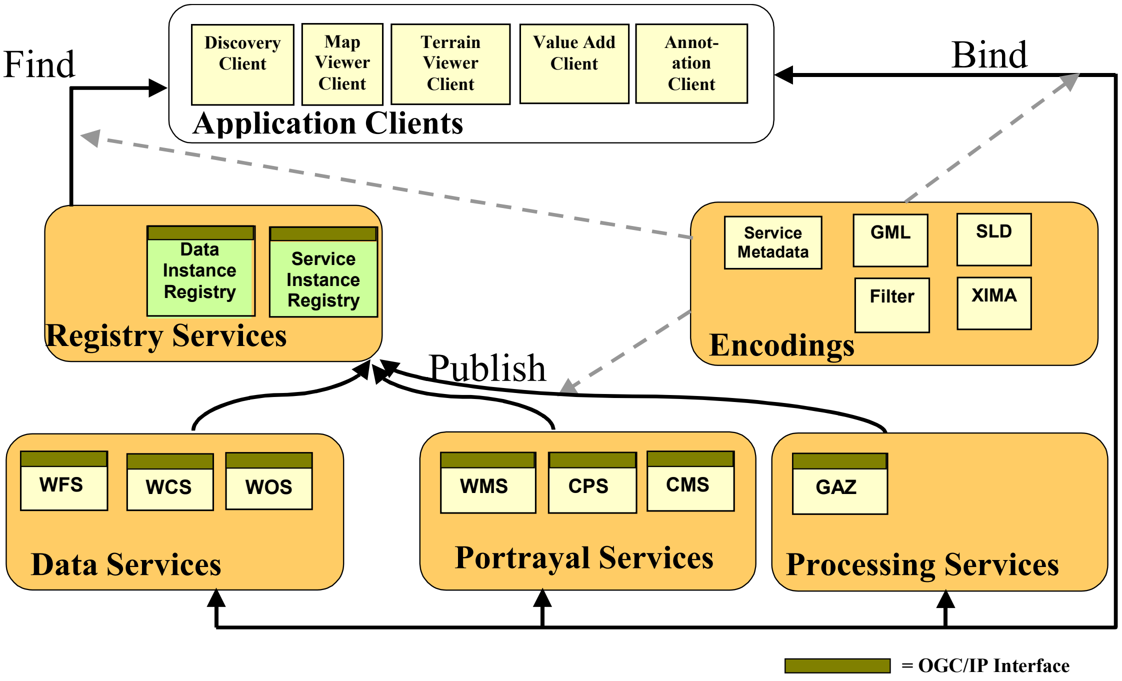

Figure 2. Open GIS Service Framework elements for CIPI-1

The CICE is designed to meet the following purposes:

- Provide a framework for coordinated development of new and extended services
- Enable interoperable services through standard interfaces and encodings
- Support publishing, discovery and binding of services through service metadata
- Allow separation of data instances from service instances
- Enable use of a provider's service on another provider's data
- Define a framework that can be implemented in multiple ways

2.2.1 Human Interaction Services

Critical Infrastructure Protection services are accessible from Application Services operating on user terminals (e.g. desktop, notebook, handset, etc.) or servers that have network connectivity. Users may use Application Services to access Registry, Portrayal, Processing and Data Services, depending upon the requirements and designed implementation of the application. Application Services commonly, but not necessarily, provide user-oriented displays of geospatial content and support user interaction at the user terminal.

Note: The Portrayal, Data, and Registry Services described below work on a client/server model. In the simplest case, the client can be a standard Web browser. To be useful, a more robust client, capable of building the service requests and processing the responses is desired. Most SCOTS software vendors provide clients for this purpose. Deploying clients for each service on *every users' workstation, however, would create a management and operations nightmare. What is needed is a single client, supporting all of the services, that is easy to manage and maintain.*

The Server Based Client addresses this issue. Server Based Clients combine the client role for Web services into a single package. This package resides on a workgroup server where users can access it through their Web browser. Being server resident, there is only one copy of the package that has to be managed and maintained. Users are presented with a single environment that combines all of the Framework functionality and hides from them the underlying complexity.

While most SCOTS vendors provide Server Side Clients or the components to build one, there is no specification for Server Side Clients. Their design is governed by the OpenGIS® specifications they implement and the operational needs of the users. This frees developers to reuse SCOTS components in a way that best meets their needs.

Discussion of the specific mechanisms for distribution and transparency of interactions between application clients and services is discussed in the Engineering Viewpoint.

Examples of CIPI applications services include:

2.2.1.1 Web Map View Client

Relevant Specifications: TBD

A Web Map Viewer Client can issue GetMap requests for different maps to several independent Web Map Servers. If each map has the same geographic area and physical dimensions, and if their backgrounds are transparent, then they can be overlaid in a single window to produce a combined map. For example, server A might produce a topography image, server B a map of rivers and lakes, and server C a map of watershed boundaries. Each server maintains the type of data in which it specializes, but the end user can obtain a combined presentation of the three Layers.

2.2.1.2 Terrain Viewer Client

Relevant Specifications: TBD

Terrain Viewer Clients are the class of applications that can exploit three dimensional terrain data. Examples of these clients are applications that support cross-country mobility, mission planning, and mission rehearsal activities.

2.2.1.3 Annotation Client

Relevant Specifications: TBD

An Annotation Client is an extension of the Map Viewer Client. Through the Annotation Client, users can view map and imagery data, create annotations features for that data, associate the annotations with discrete geographic coordinates, and store the annotations and associations back to an Annotation Server.

2.2.1.4 Discovery Client

Relevant Specifications: TBD

A Discovery Client provides the tools to enable the user to build services or data queries, issues those queries to the appropriate registry(s) and display the returned result set.

2.2.1.5 Value Added Client

Relevant Specifications: TBD

Value-Add Clients are a class of Application Service specializing in supporting the ability for users to collect and submit user input that augments geospatial information originally supplied by a data producer. Value-Add Application Services support augmentation of datasets by creating new features, and updating or deleting existing features. Value-Add Application Services typically support human interaction controls, the ability to add and remove layers, and the ability to create, select, and display cartographic styles to support of the value-adding process. Value-Add Application Services may also support the ability to draw on a background map and insert this content into a LOF or save updates to repositories and databases using OpenGIS Data Services such as WFS and WCS.

2.2.2 Registry Services

CIPI registry services provide a common mechanism to classify, register, describe, search, maintain and access geospatial information about resources available on a network. Resources are network addressable instances of typed data or services. Types of registries are differentiated by their role such as registries for cataloging data types, online data instances, service types and online service instances.

2.2.2.1 Catalog Services

Relevant Specifications: *OpenGIS® Catalog Service version 1.1*

The OpenGIS® Catalog Service Interface Specification defines a common interface that enables diverse but conformant applications to perform discovery, browse and query operations against distributed and potentially heterogeneous catalog servers. Spatial Catalog servers typically contain metadata about spatially referenced information such as maps, schematics, diagrams, or textual documents. The specification uses metadata and spatial location to identify and select layers of interest, and provides for interoperability in catalog update, maintenance, and other Librarian functions. The specification is designed for catalogs of imagery, geospatial information, and mixtures of the two. (Future versions of the specification may also support services.) It specifies open APIs that provide discovery services, access services and interfaces for catalog managers, including a complete Catalog Query Language. Detailed implementation guidance is provided for establishing and ending a stateful catalog session to: query the catalog server properties, check the status of a request, cancel a request, issue a query, present the query results, and get the schema of a discovered collection.

2.2.2.2 Secure Catalog Services

Relevant Specifications: *OpenGIS® Catalog Service version 1.1*

This class extends the Catalog class by adding Authentication and Identification to the interface, and Discretionary Access Controls (DAC) to the data management logic. All other Catalog subclasses can also be subclassed off of the Secure Catalog class.

2.2.2.3 Data Registry Service

Relevant Specifications: *OpenGIS® Catalog Service Implementation Specification, version 1.1, OpenGIS® Web Registry Service IPR (03-024)*

The Data Registry Service extends the Stateless Catalog by providing a base schema and management interfaces (create, update, and delete) to support the discovery of data providers.

2.2.2.4 Service Registry Service

Relevant Specifications: *OpenGIS® Catalog Service Implementation Specification, version 1.1, OpenGIS® Web Registry Service IPR (03-024)*

The Services Registry Service extends the Stateless Catalog by providing a base schema and management interfaces (create, update, and delete) to support the discovery of Web Services.

2.2.3 Processing Services

CIPI processing services operate on geospatial data and provide “value-add” services for applications. They can transform, combine, or create data. Processing Services can be tightly or loosely coupled with other services such as Data and Portrayal Services. Processing Services can be sequenced into a “value-chain” of services to perform specialized processing in support of information production workflows and decision support. Examples of OSF processing services include:

2.2.3.1 Gazetteer Services

Relevant Specifications: *OpenGIS® Web Feature Server version 1.0, OpenGIS® Gazetteer Service discussion paper*

1. A Gazetteer Service is a network-accessible service that retrieves the known geometries for one or more features, given their associated well-known feature identifiers (text strings), which are specified at run-time through a query (filter) request. The identifiers are any words or terms that describe the features, which are well known to the Gazetteer Service, such as a set of place names and/or landmarks. Each instance of a Gazetteer Service has an associated

vocabulary of identifiers. Thus, a Gazetteer Service may apply to a given region, such as a country, or some other specialized grouping of features. The returned geometries are expressed in an OGC Spatial Reference System according to the ISO feature model, encoded in GML.

2.2.4 Portrayal Services

CIPI portrayal services provide visualization of geospatial information. Portrayal Services are components that, given one or more inputs, produce rendered outputs (e.g., cartographically portrayed maps, perspective views of terrain, annotated images, views of dynamically changing features in space and time, etc.). Portrayal Services can be tightly or loosely coupled with other services such as Data and Processing Services and transform, combine, or create portrayed outputs. Portrayal Services may use styling rules specified during configuration or dynamically at runtime by Application Services. Portrayal Services can be sequenced into a “value-chain” of services to perform specialized processing in support of information production workflows and decision support. Examples of OSF portrayal services include:

2.2.4.1 Web Map Servers

Relevant Specifications: *OpenGIS® Web Map Server version 1.1*

A Web Map Server (WMS) generates "pictures" of georeferenced data. Independent of whether the underlying data are simple features (such as points, lines and polygons) or coverages (such as gridded fields), the WMS produces an image of the data that can be directly viewed in a graphical web browser or other picture-viewing software. A WMS labels its data as one or more "Layers," each of which is available in one or more "Styles." Upon request a WMS makes an image of the requested Layer(s), in either the specified or default rendering Style(s). The image request, called GetMap, indicates the Spatial Reference System (SRS) and Bounding Box of the portion of the Earth to be mapped, and the output width, height and format of the picture. Typical output formats include Portable Network Graphics (PNG), Graphics Interchange Format (GIF), Joint Photographic Expert Group format (JPEG), and Tagged Image File Format (TIFF). When the data do not cover the entire field of view (such as a network of roads that includes the space between the roads), the background can be made transparent in some output formats.

2.2.4.2 Secure Web Map Servers

Relevant Specifications: *OpenGIS® Web Map Server version 1.1*

This class extends the Web Map Server class by adding Authentication and Identification to the interface, and Discretionary Access Controls (DAC) to the data provider logic. All other Web Map Service subclasses can also be subclassed off of the Secure Web Map Server class.

2.2.4.3 Styled Layer Descriptor Web Map Servers

Relevant Specifications: *OpenGIS® Web Map Server version 1.1,* *OpenGIS® Style Layer Descriptor discussion paper*

An extension of the basic Web Map Server is the Styled Layer Descriptor (SLD) Web Map Server. The SLD enabled WMS inherits all of the attributes from the Web Map Server then adds support for the use of Styled Layer Descriptor documents to specify styling. Instead of generating maps of particular named layers in one or more predefined styles, an SLD Map Server extracts features from a data provider and renders them using a stylistic description encoded in XML.

2.2.4.4 Cascading Map Servers

Relevant Specifications: *OpenGIS® Web Map Server version 1.1,*

OpenGIS® Style Layer Descriptor discussion paper

The Cascading Map Server is a special case of the Web Map Server in that it does not hold any data of it's own, rather it serves as a gateway for other data providers, both OGC and non-OGC compliant. Cascading Map Servers incorporate clients for a number of services. These clients, however, do not have to be just for OpenGIS® interfaces. Legacy data providers can be accessed, their data retrieved, adjusted, and re-presented through the OpenGIS® Web Mapping Service interface. As such, the Cascading Map Server can serve a key role in presenting legacy data that may otherwise be inaccessible.

2.2.4.5 Web Terrain Servers

Relevant Specifications: *OpenGIS® Web Terrain Server discussion paper*

The Web Terrain Server extends the Web Map Server (WMS) interface to allow the portrayal three dimensional geospatial data. This service can be exploited to perform tasks such as terrain analysis, mission planning, and fly-throughs.

2.2.5 Data Services

OSF data services provide access to collections of data in repositories and databases. Resources accessible by Data Services can generally be referenced by a name (identity, address, etc). Given a name, Data Services can then find the resource. Data Services usually maintain indexes to help speed up the process of finding items by name or by other attributes of the item. The sections below describe the current OSF set of Data Services. Examples of OSF data services include:

2.2.5.1 Web Feature Server

Relevant Specifications: *OpenGIS® Web Feature Server version 1.0*

The Web Feature Service (WFS) supports the query and discovery of geographic features. In a typical Web-base scenario, Web Feature Service (WFS) delivers GML (XML) representations of simple geospatial features in response to queries from HTTP clients. Clients (service requestors) access geographic feature data through a WFS by submitting a request for just those features that are needed for an application. The client generates a request posts it to a WFS instance (a WFS server on the Web). The WFS instance executes the request, returning the results to the client (service requester) as GML. A GML-enabled client can manipulate or operate on the returned features.

2.2.5.2 Secure Web Feature Server

Relevant Specifications: *OpenGIS® Web Feature Server version 1.0*

This class extends the Web Feature Server class by adding Authentication and Identification to the interface, and Discretionary Access Controls (DAC) to the data provider logic. All other Web Feature Service subclasses can also be subclassed off of the Secure Web Feature Server class.

2.2.5.3 Web Feature Server – Transactional

Relevant Specifications: *OpenGIS® Web Feature Server version 1.0*

The Transactional Web Feature Server extends the base WFS class with enhancements to allow the client to insert, update, and delete data.

2.2.5.4 Web Annotation Server

Relevant Specifications: *OpenGIS® Web Annotation Server discussion paper*

The Web Annotation Server extends the Web Feature Server (WFS) interface to allow users to create annotation features, associate them with vector and/or imagery features, and store them back to the server. Stored annotations can retrieved and evaluated in the context of the original features and/or with other information georeferenced to the same area.6.3.5.4 Web Coverage Server.

2.2.5.5 Web Coverage Server

Relevant Specifications: *OpenGIS® Web Coverage Server discussion paper*

The Web Coverage Services (WCS) allows access to geospatial "coverages" containing values or properties of geographic locations, rather than static maps (server-rendered as pictures). In a typical Web-based scenario, Web Coverage Services delivers coverage data (e.g., images or DTED) in response to queries from HTTP clients. Access to intact (unrendered) geospatial information is needed for client-side rendering, multi-valued coverages, and input into scientific models and other clients beyond simple viewers. The WCS interface supports delivery of images, multi-spectral imagery, elevation data (e.g., DTED) and other scientific data.

2.3 Information Security

2.3.1 Registration Authority

Relevant Specifications: see IETF X.509 Public Key Working Group (PKIX)

Authentication and Identification within the CICE will be accomplished through Public Key cryptology. Public Key cryptology uses a private key (known only to the user) and a public key known to everyone. Anything encrypted with a private key could only have been encrypted by the owner of that private key. Likewise, anything encrypted with the public key can only be decrypted with the private key (i.e. the owner). Public Key Infrastructures use these public/private key pairs to perform Identification and Authentication. But who assures that the owner of a private key is who they claim to be?

Registration Authorities are responsible for assuring that the owner of a private key is who they claim to be. In most cases the Registration Authority is the body that issues the key pairs. The degree of assurance a private key has depends on how rigorous the Registration Authority is in verifying the identity of a key requestor.

2.3.2 Certificate Authority

Relevant Specifications: see IETF X.509 Public Key Working Group (PKIX)

Certificate Authorities (CA) are responsible for providing public keys for individuals and assuring the association between that individual and the key. CAs will usually be set up based on an individual's organization, FEMA for example can be expected to set up a CA. The local security policy determines which CAs to trust. A user certificate coming from an "untrusted" CA can be rejected.

2.3.3 Security Profile Manager

Relevant Specifications: see IETF X.509 Public Key Working Group (PKIX)

Due to the large population of potential users of CIPI data, security policies must be based on the user's role and credentials, not on their ID. Yet the role and credentials data must be available to the service in a trusted fashion. A Security Profile Manager (SPM) is the authoritative source for this information. Each emergency responder will have a "home" SPM where all of the information about their clearances, roles and authorizations will reside. Access to these directories will be through an LDAP interface. This interface will be protected with authentication and encryption. Access to the credentials data for a single individual will require a valid certificate for that individual. These directories will be maintained by the same organizations that investigate and assign the credentials to that individual.

2.4 CICE Service Interactions

The "Cross Border Project" system concept, introduced in Section 6 (CICE Use Case Narratives) of the Enterprise Viewpoint, is used here to describe the role of CICE OpenGIS Web Services, their interfaces and interactions. In this scenario a commercial chemical truck is suspected to be leaking chlorine gas as it approaches a national border crossing in an urban area (e.g., Ambassador Bridge between Windsor, Canada and Detroit in the US). The truck may have been hijacked.

Within this scenario there are a large number of actors potentially involved: Emergency Operations Centers (EOC) operating at national, state and local levels, national emergency agencies, first responders, authorized responders, municipal police, police dispatchers (PD), Hazardous Materials Response Teams (HMRT), Threat Assessment Teams (TAT), Public Alerting System Coordinators (PASC), print and broadcast media, etc.

This scenario is one of situation management and alerting involving multiple governmental agencies at multiple levels (international, national, state, local) and private sector. This scenario describes a typical set of activities that might occur within an Emergency Operations Center (EOC). It is only a narrow glimpse into the full set of activities that occur before, during and after such incidents by the full range of actors involved in disaster planning, detection, management, communication, response and recovery.

The situation management and alert notification process that occurs within an EOC is a series of steps that form a continual closed loop that may occur, depending on the nature of the incident, in the span of minutes, hours or days. The process can be described in five steps depicted in Figure 3:

1) Detect event and establish geographic context,

2) Notify emergency responders,

3) Develop situation awareness,

4) Develop response plan,

5) Assess risks and package information.

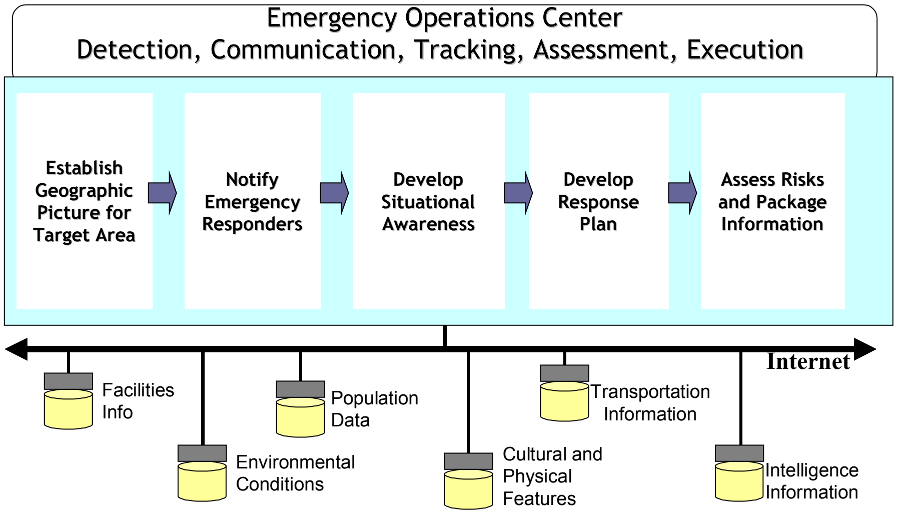
Emergency Operations Center
Detection, Communication, Tracking, Assessment, Execution
Establish Geographic Picture for Target Area
Notify Emergency Responders
Develop Situational Awareness
Develop Response Plan
Assess Risks and Package Information
Internet
Facilities Info
Environmental Conditions
Population Data
Cultural and Physical Features
Transportation Information
Intelligence Information

Figure 3. An Emergency Response Process

Datasets required for effective conduct of the emergency response process include:

- Orthoimagery,
- Transportation,
- Borders (national, state/provincial, local)
- Cadastral (Parcel Boundaries and Building Footprints)
- Natural Features (Terrain, Hydrography, etc)
- Critical Infrastructure (aquifers, water distribution, water treatment, bridges, tunnels, gas mains, geodetic control, telecommunications, power generation and transmission, public assembly, hospitals, hazardous materials storage, etc)
- Demographics (population distribution and density, economic activities, etc)
- Weather (local/national, current/forecast)

The following series of sequence diagrams are used to elaborate the role of various types of OpenGIS Web Services and the nature of the interactions between client applications, such as an EOC Client, and services comprising the CICE as required for the cross-border situation management and alert notification scenario.

Activity #1: Establish Geographic Context

The objective of this activity is to develop a base map showing the location of the incident and its surrounding vicinity including roadway, waterway and border-crossing data. This information is to be used by Hazardous Materials Response Team (HMRT) and Police Dispatchers (PD).

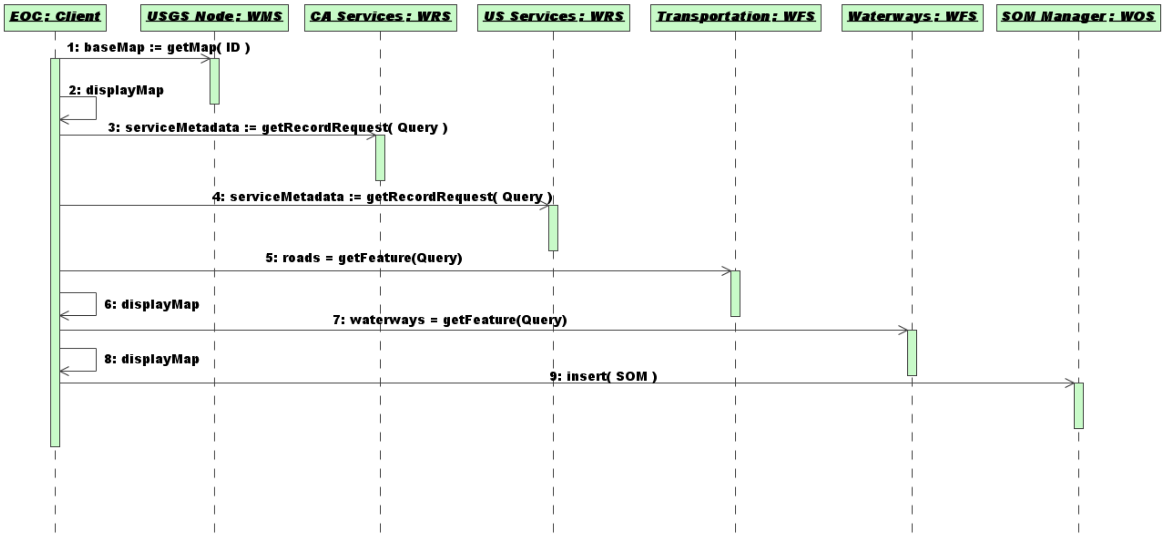
EOC : Client
USGS Node : WMS
CA Services : WRS
US Services : WRS
Transportation : WFS
Waterways : WFS
SOM Manager : WOS
1: baseMap := getMap(ID)
2: displayMap
3: serviceMetadata := getRecordRequest(Query)
4: serviceMetadata := getRecordRequest(Query)
5: roads = getFeature(Query)
6: displayMap
7: waterways = getFeature(Query)
8: displayMap
9: insert(SOM)

Figure 4. Set Geographic Context

Steps 1-2. The EOC Client first accesses instances of OWS WMS (such as the USGS Node), to gather basemap data including orthoimagery, transportation and basic cultural features for the area of interest.

Steps 3-4. For more detailed and current information, the EOC Client queries the service registries (WRS), maintained and operated by USGS and Geoconnections portals, for services that offer appropriate transportation and waterway information.

Step 5-8. Having found services with the appropriate data for the current situation, the EOC Client proceeds to access and present those data to the user in the form of a map.

Step 9. EOC Client creates a “Situation Object Model” (SOM) document for the present situation and inserts it as an entry in the SOM Manager. The information gathered in this activity is now available to all user(s) with the appropriate access privileges.

Activity #2: Communicate

The objective of this activity is to identify and map the major roadways, including border crossings, leading toward and away from the incident location. The EOC Client must first upload the initial situation picture (developed in Activity #1) and then communicate alert messages to the appropriate responders.

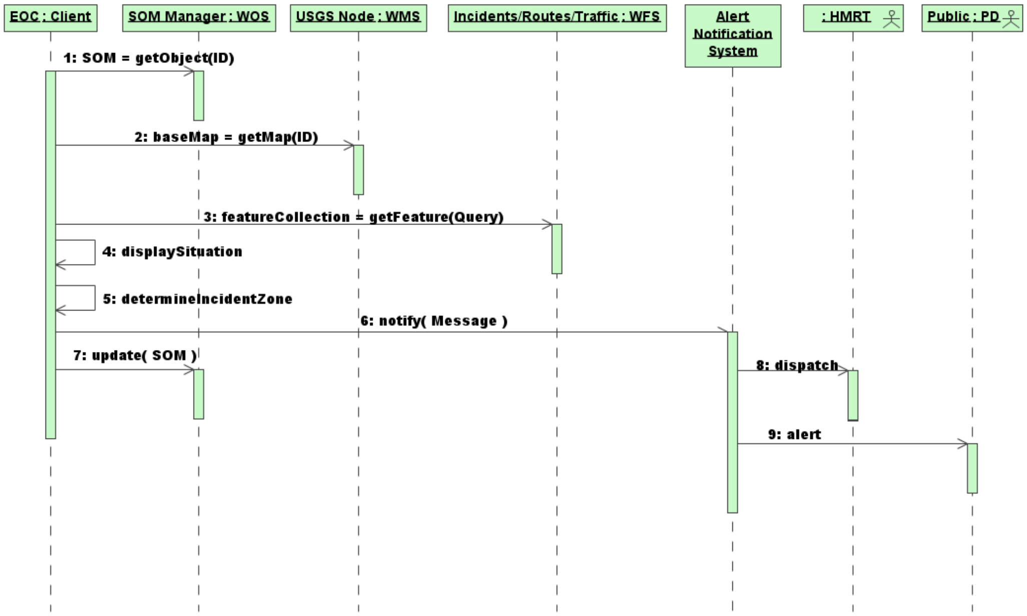

Figure 5. Alert Notification

Steps 1-4. EOC Client accesses the SOM document and subsequently various web services to access and display basemap data (developed in Activity #1), incident location, routes and traffic information that together represent the current “situation picture”.

Step 5. The user of the EOC Client or through interaction with other EOC actors and services, determines the incident zone (i.e., the area-of-interest and region of operations for the incident).

Step 6,8,9. The EOC Client asynchronously notifies the Alert Notification System responsible for packaging and communicating alert notifications to appropriate authorized response personnel (Fire and Rescue, HMRT, Police, etc).

Step 7. EOC Client updates the SOM document entry in the SOM Manager with the latest information associated with the incident. The information gathered in this activity is now available to all user(s) with the appropriate access privileges.

Activity #3: Track and Report Situation

The objective of these activities is to track and map the location of incident subjects (e.g., vehicles) as reported in real-time based on the closest mile marker or intersection location.

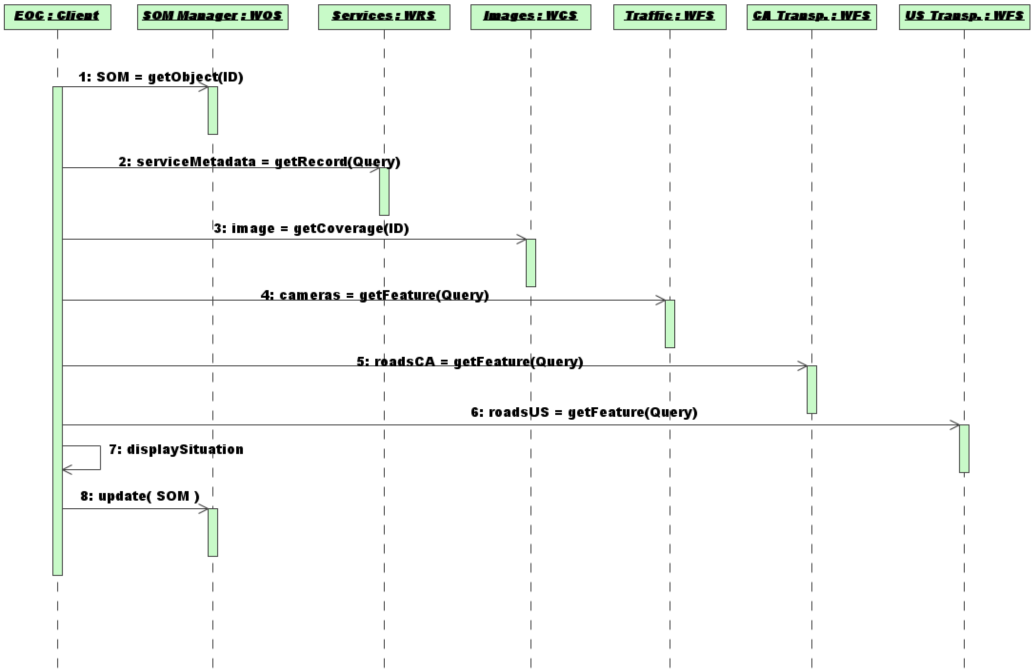

Figure 6. Track and Report Situation

Step 1. EOC Client accesses the SOM document and subsequently various web services to access and display basemap data and the current "situation picture" (developed in Activities #1-2).

Step 2. EOC Client accesses the Services WRS to find and subsequently access services having appropriate information, including: high-resolution imagery showing major roads leading to and away from the bridge and tunnel at the border crossing, traffic cameras, large scale road datasets, and the current observed/detected position of the vehicle of interest.

Steps 3-7. EOC Client accesses services discovered in Step 2 to obtain current/relevant imagery, traffic situation camera images, detailed road network data (for both sides of border), and incident location and related features. EOC Client displays this situation information in one or more views (maps, reports, etc).

Step 8. EOC Client updates the SOM document entry in the SOM Manager with the latest information associated with the incident. The information gathered in this activity is now available to all user(s) with the appropriate access privileges.

Activity #4: Plan Evacuation

The objective of this activity is to track and map the final location of the vehicle as reported in real-time and generate evacuation routes for the population within the affected area of the incident.

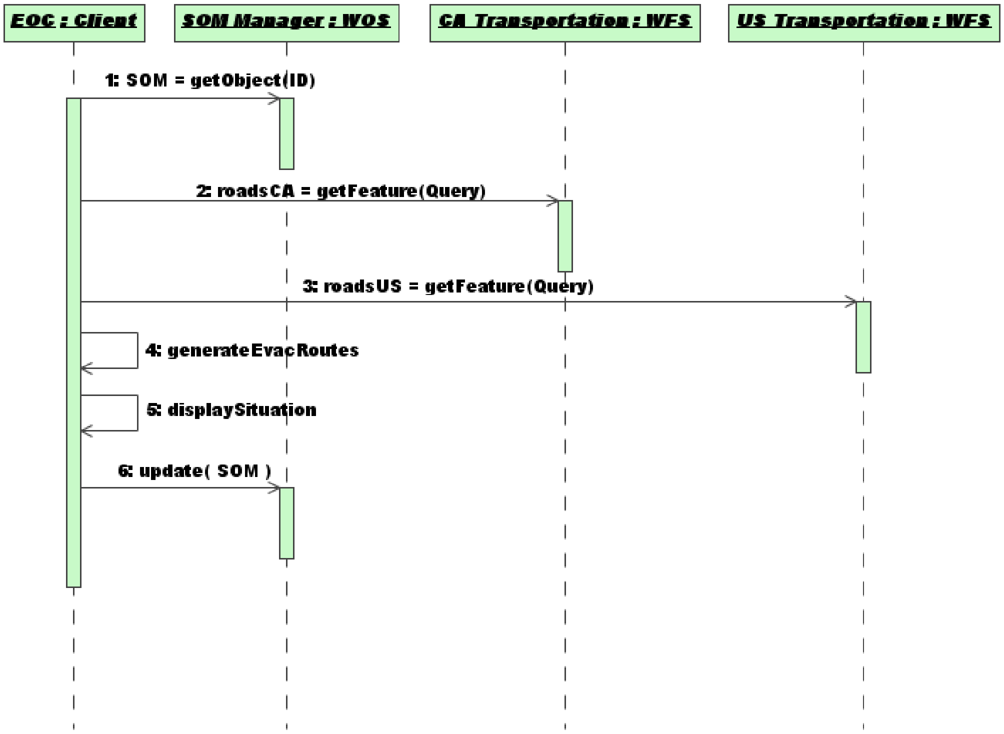

Figure 7. Evacuation Planning

Step 1. EOC Client accesses the SOM document and subsequently various web services to access and display basemap data and the current "situation picture" (developed in Activities #1-3).

Step 2-3. EOC Client accesses large scale road datasets, from appropriate authorities, for jurisdictions on both side of the national border.

Steps 4-5. EOC Client, by automated or semi-automated means, identifies emergency evacuation routes using data acquired in Steps 2-3 and in earlier Activities #1-3. EOC Clients display these evacuation routes as a layer overlaid on the base map.

Step 6. EOC Client inserts the generated emergency evacuation routes to the SOM document and updates the SOM document entry in the SOM Manager. The information gathered in this activity is now available to all user(s) with the appropriate access privileges.

Activity #5: Risk Assessment and Information Packaging

The objective of this activity is to: 1) map structures and population, 2) display HAZMAT plume data illustrating the (potential) impact of the chemical release to the structures and population within the vicinity of the incident, 3) link the situation to specific actions (e.g., public alert, evacuation, recovery operations, etc) to the threat source and 4) package for distribution.

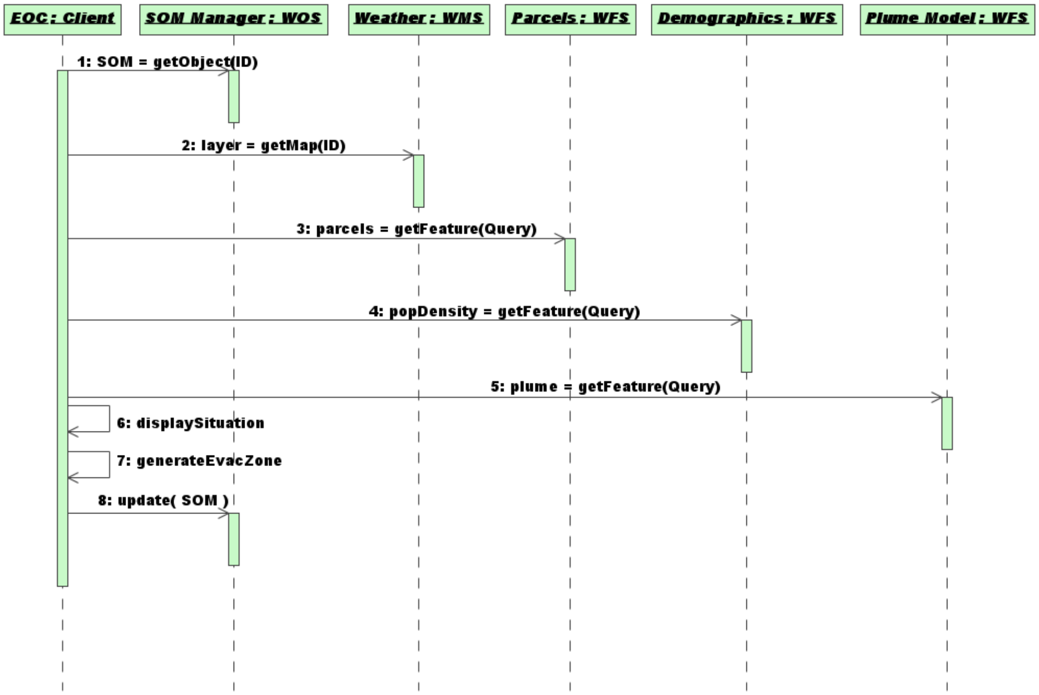

Figure 8. Risk Assessment

Step 1. EOC Client accesses the SOM document and subsequently various web services to access and display basemap data and the current "situation picture" (developed in Activities #1-3).

Steps 2-6. Assess risk by accessing and visualizing: a) weather data, b) population information (e.g., parcels, buildings and population densities) and c) plume data calculated from a point-source chemical dispersion model.

Step 7. Package this information in the form of an Evacuation Zone map suitable for public release through the print and broadcast media.

Step 8. EOC Client inserts the collected information into the SOM document and updates the SOM document entry in the SOM Manager. The information gathered in this activity is now available to all user(s) with the appropriate access privileges.

Bibliography

[1] IETF/RFC 2119. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997. Available [online]: <http://www.ietf.org/rfc/rfc2119.txt>.