CubeWerx USA

US Army Corps of Engineers®

2008 NSDI Cooperative Agreement Program

Category 2: Best Practices in Geospatial Service Oriented Architecture (SOA)

Best Practices for Role-based Access Control in Geospatial SOA

Final Report
Version 0.9

Presented to:

NSDI

November 30, 2009

Table of Contents

NSDI Cooperative Agreements Program

Category 2: Best Practices in Geospatial Service Oriented Architecture (SOA)

Final Report

Date: November 30, 2009

Agreement Number: 08HQAG0059

Project title: Role-based Access Control - Best Practices in Geospatial SOA

Organization:
CubeWerx USA™
12052 Willowood Drive
Lake Ridge, VA 22192
Internet Address: www.cubewerx.com

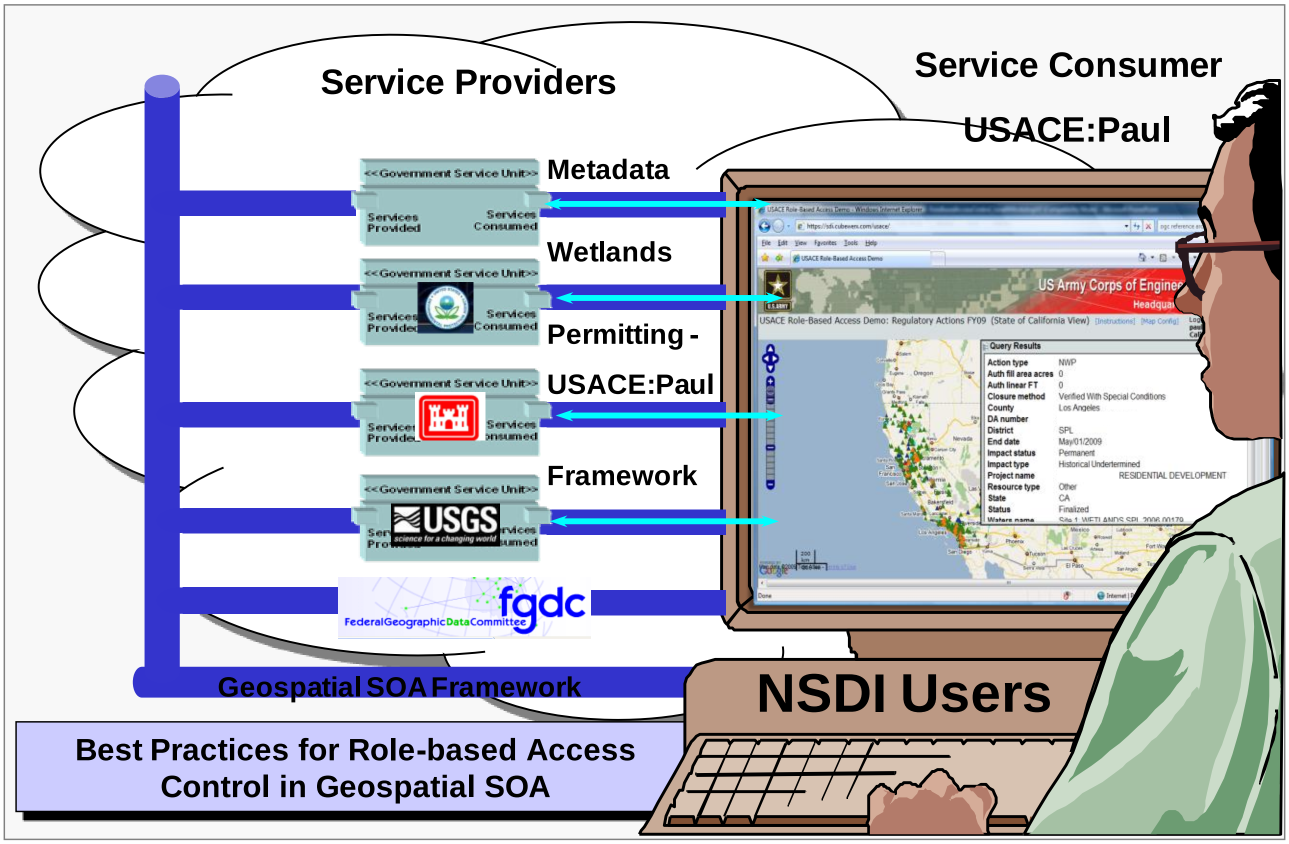
Project Leader:
Jeff Harrison
CubeWerx
Phone: 703.628.8655, jharrison@cubewerx.com
Internet Address: http://www.cubewerx.com

Collaborating Organizations:
Glenn Stowe
CubeWerx
Phone: 819.771.8303, gstowe@cubewerx.com
Internet Address: http://www.cubewerx.com

Joel Schlagel, Institute for Water Resources
U.S. Army Corps of Engineers
Phone: 603.646.4387, Joel.D.Schlagel@usace.army.mil
Internet Address: http://www.usace.army.mil

Executive Summary

This project has developed Best Practices for one of the most important, but least understood, areas of Geospatial SOA – Role-based Access Control. Development was coordinated with other 2008 Category 2 recipients and satisfies multi-agency requirements through the modeling and deployment of business processes and related geospatial service components. These Best Practices will help the NSDI to shed rigid and inward-looking approaches and transform into a more agile, responsive and customer-centric framework driven by collaborative partnerships. Of particular interest was the advancement of technology to support regulatory interoperability between organizations like USACE, EPA and others.


Service Providers
Service Consumer
USACE:Paul
<<Government Service Unit>>
Services Provided
Services Consumed
Metadata
Wetlands
Permitting - USACE:Paul
Framework
USGS
science for a changing world
fgdc
FederalGeographicDataCommittee
Geospatial SOA Framework
NSDI Users
US Army Corps of Engineers
USACE Role-Based Access Demo: Regulatory Actions FY09 (State of California View)
Query Results
Best Practices for Role-based Access Control in Geospatial SOA

This effort is important because Geospatial SOA based on OGC® and other standards are strongly influencing development of the Federal Enterprise Architecture (FEA) Geospatial Profile[1], especially data access and update. These efforts have matured to a point where broad acceptance is now dependent on the capacity to secure data resources. In fact, organizations like USACE that are considering participation in the NSDI must also consider how they can establish distributed security frameworks for role-based access control to SOA resources. These requirements will continue to increase as data access transitions into data management with services like GeoSynchronization and Web Feature Server- Transactional (WFS-T) where loosely affiliated parties collaborate on maintenance of shared geospatial data resources.

Specifically, the lack of adequate Access Control solutions have contributed to a situation where many organizations have been avoiding deployment of their OGC services like WFS-T on the Web. The lack of such controls has forced data providers to adopt data sub-setting techniques to isolate access to geospatial data based on different projects, users, groups of users, etc. But such approaches have been proven to add hardware, software, implementation and maintenance costs for organizations deploying their OGC-based Spatial Data Infrastructure (SDI) services on standalone servers or cloud computing platforms.

To meet this challenge, this project defined and documented Best Practices in Geospatial SOA for Role-based Access Control. This project leveraged CubeWerx and OGC investments in developing solutions to solve this important security challenge. The capability was deployed as part of a distributed SOA laboratory for Services Development, Test, and Evaluation (DT&E) designed to drive out Best Practices. Rather than dictating policies, the goal was to support policies already available in most organizations and provide secure, flexible, extensible components for supporting SDI Access Control Rules (SACR). These components were invoked in open geospatial web services, allowing the simulation of trusted organizations in a federation, reuse of existing authentication methods and definition of new access control rules. Scenarios ranging from a hurricane response along the Gulf coast, cross-border information sharing, and regulatory permitting were executed and common Use Cases derived.

The resulting Access Control Rules were defined in an XML Schema using an XML file that can be dynamically parsed by OGC-compliant Web services. With this approach Authentication services can provide access control on a user-by-user basis. For example, several rules can be specified in an <AccessControlRules> document, where each rule can apply to a different set of usernames, groups and/or roles.

The approach modeled in this project is compatible with IT industry-wide efforts working on "Identity Metasystems", OASIS security standards for Information Cards, and the Web Services Protocol Stack that includes WS-Security, WS-Trust, WS-MetadataExchange and WS-SecurityPolicy. In particular, this *Best Practice for Role-based Access Control* adopted the philosophy of using Authentication methods defined by IT industry-wide efforts and focused on defining reusable *SDI Access Control Rules* for granting access to OGC services by role, geographic extent, feature and SDI operations. This approach adds significant new capability for deploying service components by allowing organizations to optimize data services and reduce costs.

While the project demonstrates certain functionality specific to USACE's needs, it also demonstrates capabilities that have value across all application and geospatial data stewardship domains, and provides a strong foundation for the NSDI and Geospatial Line of Business (LoB) across the government.

Project Narrative

Introduction and Background

This document outlines Best Practices for one of the most important, but least understood, areas of Geospatial SOA and Geospatial Cloud Computing – Role-based Access Control. Development of these Use Cases was coordinated with other 2008 Category 2 recipients and helps satisfy multi-agency requirements through the modeling and deployment of business processes and related data and service components. Documentation of these Best Practices also helps the National Spatial Data Infrastructure (NSDI) shed rigid and inward-looking approaches and transform into a more agile, responsive and customer-centric framework driven by collaborative partnerships. Of particular interest was the advancement of technology that can support regulatory data interoperability between organizations like USACE, EPA and USFWS.

This effort is important because Geospatial SOA based on OGC® and other standards are strongly influencing development of the Federal Enterprise Architecture (FEA) Geospatial Profile[1], especially data access. These efforts have matured to a point where broad acceptance is now dependent on the capacity to secure data resources. In fact, organizations like USACE that are considering participation in the NSDI must also consider how they can establish distributed security frameworks for role-based access control to SOA resources. These requirements will continue to increase as data access transitions into collaborative data management with services like the Web Feature Server- Transactional (WFS-T) and GeoSynchronization Services where loosely affiliated parties collaborate on maintenance of shared geospatial data resources.

To meet this challenge, this project defined and documented Best Practices in Geospatial SOA for Role-based Access to GeoData as a key component of USACE and NSDI Business Process requirements. This project leveraged CubeWerx's investment in developing solutions to solve this important security challenge. Specifically, CubeWerx has tested and deployed an access control framework to facilitate secure sharing web resources and manage the roles of participants in such a way that each jurisdiction/data publisher maintains autonomy of its published web-enabled data resources.

This project leveraged CubeWerx and OGC investments in developing access control frameworks to solve this important security challenge. The framework manages identities and enforces role-based access control rules on web resources. Rather than dictating policies, its goal is to support policy rules already available in most organizations and provide secure, flexible, extensible, and highly available components for supporting open Access Control Rules (ACR). These components are invoked as web services, allowing each trusted organization in a federation to determine its authentication and access control policies.

The proposed project built on this capability and designed, deployed, and documented reusable services and Best Practices for Role-based Access to GeoData within NSDI enterprises. In this project, our team provided expertise related to current trends and developments in geospatial services oriented architectures, and collaborated with the other Category 2 Awardees to identify and support common services and solutions for use across the government based on common understandings of SOA for geospatial enterprises.

[1] http://colab.cim3.net/file/work/geocop/ProfileDocument/FEA_Geospatial_Profile_v1_1.pdf

While the project demonstrates functionality specific to USACE's needs, it also demonstrates Best Practices that have value across all application and spatial data stewardship domains, and provides a strong foundation for the NSDI and Geospatial Line of Business (LoB) across the government.

SOA Definitions and Approach

The world is changing at an accelerating rate and the federal government needs to keep pace.[2] Broad-based change is always difficult, but the federal government is plagued by a variety of inhibitors to change, including vertical vs. mission organizational orientation; bureaucratic culture; budgetary cycles and processes that do not facilitate agility or reuse; and a large and diverse current technology base. Service Oriented Architecture (SOA) promises to help agencies rapidly reconfigure their business and more easily position IT resources to serve it. Improved *business agility* – through sharing and reuse of infrastructure, services, information, and solutions - is a growing requirement in the federal government today and will be increasingly critical in the future.

To address the challenge of change many federal organizations are implementing, considering or planning for a broad based adoption of SOA. In order to effectively move to an SOA environment, an organization must conduct careful planning and assessments for a variety of organizational, architectural, and technological challenges. With recent advances in federal enterprise architecture, federal chief architects and chief information officers have a deeper insight into their current IT architectures at all levels of government. In most organizations, this visibility has exposed many inefficiencies and undesirable redundancies, as well as disconnect between the promise and the reality of technology for improving business outcomes. In turn, this has led to a variety of consolidation initiatives and reengineering efforts at all levels of the federal government.

While much of this guidance is concerned with cross-agency initiatives which leverage reuse efficiencies and improved organizational performance, agencies themselves are faced with similar internal challenges. Recognizing this concern, as well as others, OMB published the Federal Enterprise Architecture (FEA) Practice Guidance [OMB, 2007b] that introduces Segment and Solution Architectures and their relationships with Enterprise Architecture (EA) through a notional framework (see Figure 1-3 of the FEA Practice Guidance document). The Solution Architecture is equivalent to an IT system that is reconciled to the Segment Architecture. The FEA Practice Guidance strongly indicates that Segment and Solution Architectures inherit their structure, policies and standards and re-usable and sharable solutions from the Enterprise Architecture. This is directly aligned with the direction of Service Oriented Architecture.

Just as industry has adopted SOA best practices, it stands to reason that federal organizations will turn to SOA best practices to optimize their IT and business architectures. SOA is not just a technology to be leveraged; it is a true paradigm shift and requires substantial organizational, cultural and management changes to be effective.

Like most technological advances, SOA leverages the technologies and standards that preceded it. The term "Service Oriented Architecture" was widely adopted when the World Wide Web Consortium (W3C) established standards for integrating business systems over the Internet through the standardized use of web technologies and protocols. The standards developed were designed to enable heterogeneous

[2] This section adapted from http://smw.osera.gov/pgfsoa/index.php/Version1.1#Introduction_.5BDocument_Section_1.5D

distributed systems to interoperate through standard web-based conventions modeled to support distributed component architectures. For the purposes of this Best Practice, we will adopt the Organization for the Advancement of Structured Information Standards (OASIS) definition for SOA -

SOA is a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains.

In this project CubeWerx USA used the initial list of commonly-used terms and their definitions and posted these to the "Confluence" project collaboration site for consideration by FGDC and the two other CAP2 award recipients. The terms and definitions were taken from authoritative sources, and the references to those sources are included in the listing. We also continued to add to the list and refine the individual definitions throughout the duration of the project, relying most heavily on the "*Practical Guide to Federal Service Oriented Architecture (PGF SOA)*" Version 1.1 Final: June 2008.

From review of the "PGF SOA" our team found it useful to view government geospatial capabilities provider organizations from the service perspective. The "government service unit" depicted in Figure 1 - Government Service Unit could represent the geospatial capabilities of an organization at any level (i.e., department, agency, bureau, program, division) or could represent a collaborative geospatial initiative such as wetland permitting that includes multiple government organizations. For the purpose of this document, we defined a ***Government Service Unit*** as –

An organization of government resources (automated systems, etc.) in the form of a standards-based online service (OGC WMS, WFS, WCS, WMTS, CS-W, GSS, etc.) providing geospatial access, discovery, processing, geosynchronization, transaction services on Internet cloud.

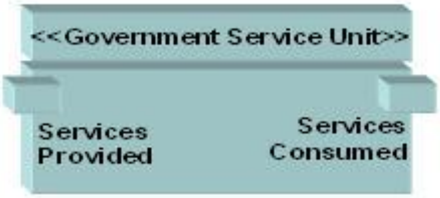


Figure 1 - Government Service Unit

Figure 2 – Government Service Unit Providers and Consumers depicts multiple geospatial government service units in a Provider-Consumer relationship. The service model applies to the services the federal government offers to its constituencies. The service model is apparent within the Federal Enterprise Architecture (FEA) Business Reference Model and the Service Component Reference Model that the Office of Management and Budget (OMB) has established as the overarching framework for understanding the business of the US federal government [OMB, 2007a]. In particular, the relationship between the Business Reference Model and the Service Component Reference Model helps agencies begin to define their specific service model as a combination of business and technology services. The service model is the core vehicle to drive Geospatial SOA adoption and implementation.

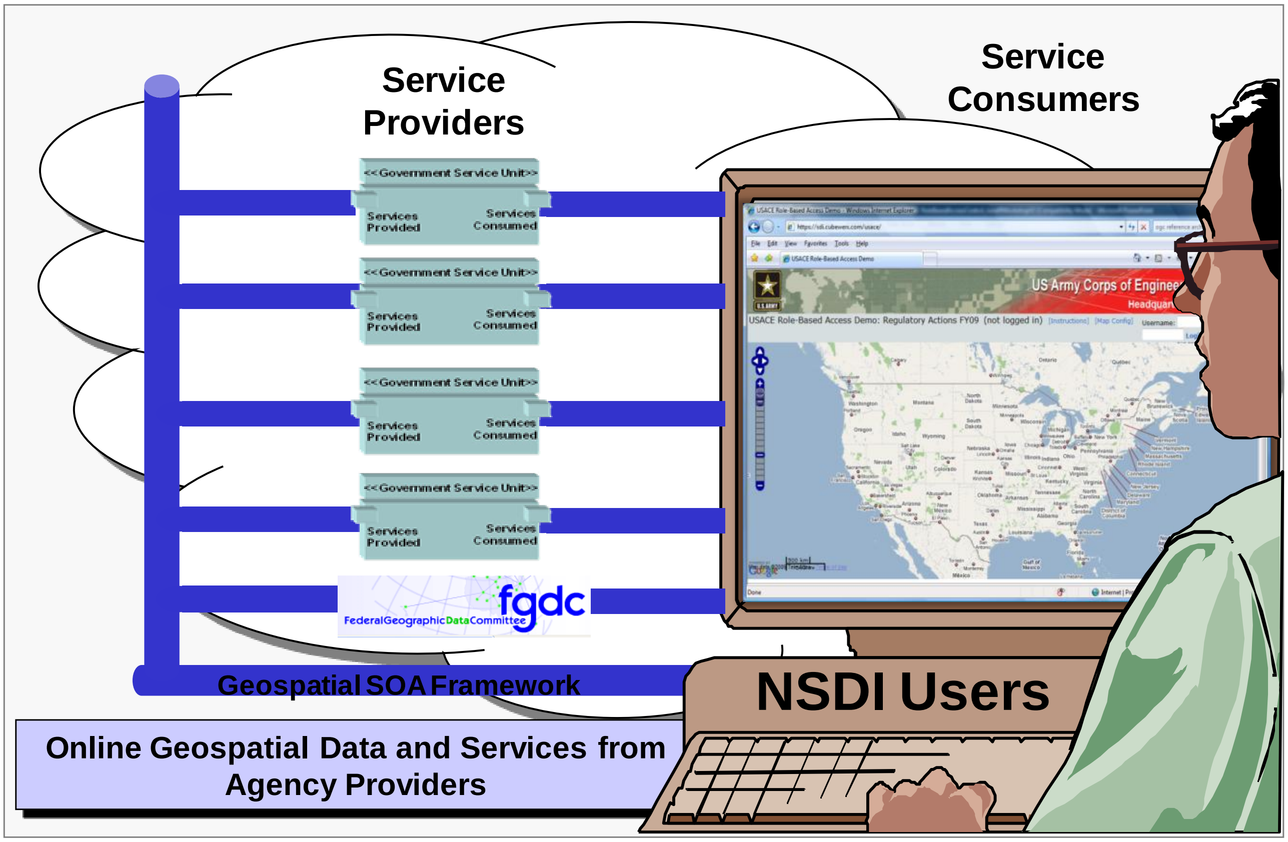

Service Providers
Service Consumers
<<Government Service Unit>>
Services Provided
Services Consumed
<<Government Service Unit>>
Services Provided
Services Consumed
<<Government Service Unit>>
Services Provided
Services Consumed
<<Government Service Unit>>
Services Provided
Services Consumed
fgdc
FederalGeographicDataCommittee
Geospatial SOA Framework
NSDI Users
Online Geospatial Data and Services from Agency Providers
US Army Corps of Engineers
USACE Role-Based Access Demo: Regulatory Actions FY09 (not logged in)

Figure 2 – Government Service Unit Providers and Consumers in Geospatial SOA.

In the Geospatial Service Provider-Consumer model agencies move from an on-premise computing model to access, discovery, processing & collaboration services on Internet cloud – leveraging shared Government Service Units.

Shared Government Service Units may be accessed to perform mission critical business processes like regulatory permitting. For example, data services supporting USACE regulatory permitting may be provided by USACE, EPA, USFWS, Geodata.gov and USGS.

However, organizations like USACE that are considering participation in an online shared NSDI must also consider how they can establish distributed security frameworks for role-based access control to SOA resources (Figure 3). These requirements will continue to increase as data access transitions into collaborative data management with services like the Web Feature Server- Transactional (WFS-T) and GeoSynchronization Services[3] where loosely affiliated parties collaborate on maintenance of shared geospatial data resources.

[3] http://www.opengeospatial.org/standards/requests/43

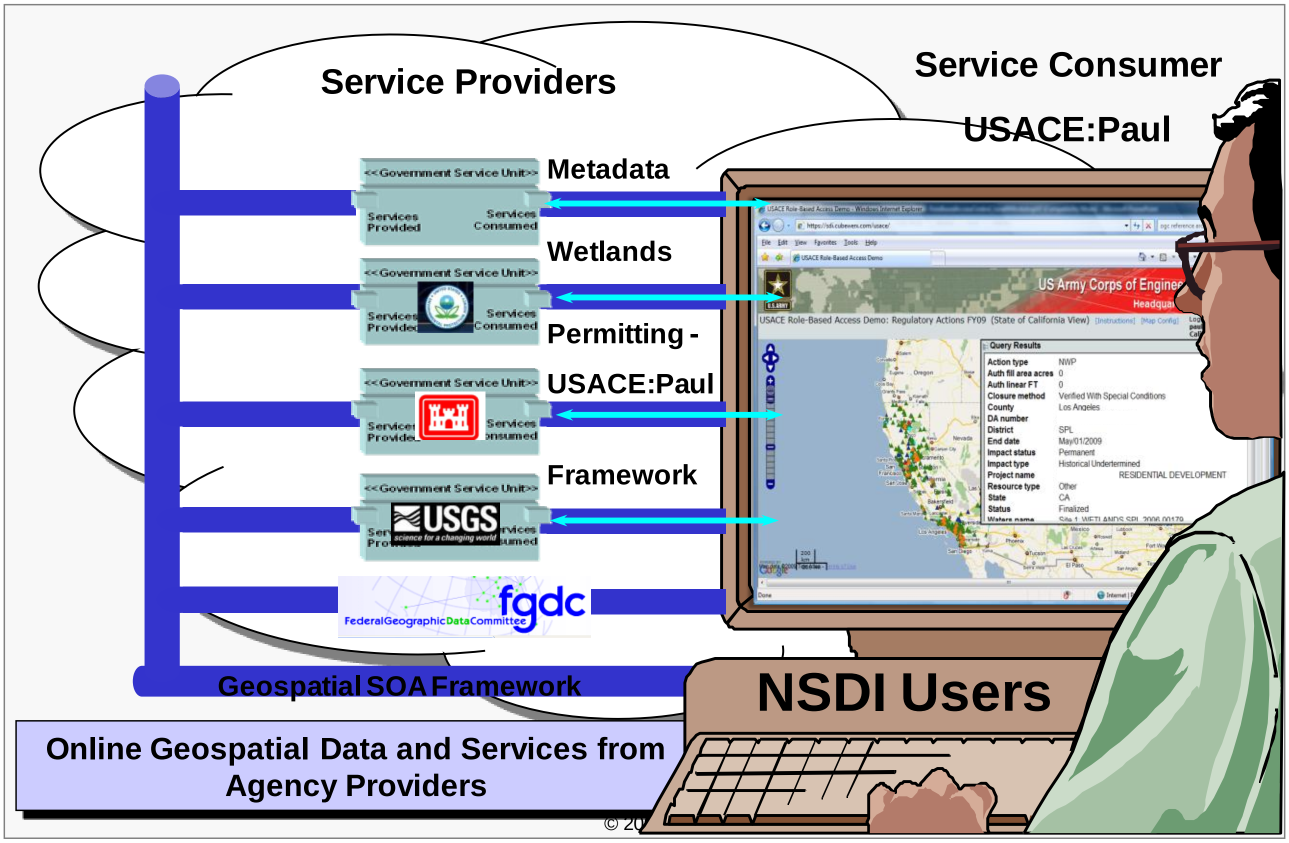

Service Providers
Service Consumer
USACE:Paul
<<Government Service Unit>>
Services Provided
Services Consumed
Metadata
Wetlands
Permitting - USACE:Paul
Framework
USGS
fgdc
Federal Geographic Data Committee
Geospatial SOA Framework
NSDI Users
Online Geospatial Data and Services from Agency Providers
US Army Corps of Engineers
USACE Role-Based Access Demo: Regulatory Actions FY09 (State of California View)
Query Results
© 20

Figure 3 - Shared geospatial Government Service Units can support business processes like regulatory permitting. In this environment role-based access control frameworks are essential.

USACE and Geospatial SOA

USACE is involved in all phases of Geospatial SOA development and deployment and brings extensive enterprise geospatial data and systems experience to this effort. Geospatial data and systems are used throughout USACE in support of planning, engineering and design, construction, operation, maintenance, and/or regulation of civil works or military construction projects, and to support USACE functional areas having responsibility for environmental investigations and studies, archeological investigations, historical preservation studies, hazardous and toxic waste site restoration, structural deformation monitoring investigations, regulatory enforcement activities, and support to Army installation maintenance and repair programs and installation master planning functions.

USACE has adopted a corporate approach to implementing geospatial technology that meets functional business process requirements in harmony with Federal, State, and local agency programs. The intent is to produce geospatial products more efficiently while serving customers. These efforts are in compliance with Executive Order (EO) 12906, Coordinating Geographic Data Acquisition and Access, and with the National Spatial Data Infrastructure and Office of Management and Budget’s (OMB) Circular A-16, Coordination of Geographic Information and Related Spatial Data Activities.

The prime goal of USACE is to advance eGIS, a shared spatial data infrastructure that will support USACE varied geospatial data needs. In order to be successful in USACE, a geographically dispersed organization, eGIS is designed as a distributed architecture where each District and Division is responsible for hosting their data. The eGIS architecture accommodates desktop, client-server, and Web-based applications. While desktop applications have historically accommodated more powerful analysis software, developing geospatial Web services and Web-based applications are maximized.

USACE believes that Geospatial SOA, Web services and Web-based applications provide the easiest means to integrate applications throughout a Division and across USACE. Open standards, such as those developed by the Open GIS Consortium (OGC) and implemented by vendors, need to be utilized to the greatest extent possible in order to maximize interoperability between systems. USACE is also implementing CorpsMap, a spatial portal that accesses a variety of existing USACE-wide databases. It is an Internet map-based display and information dissemination system for various USACE databases that have geographically based information in digital form. CorpsMap enables USACE information to be easily accessed, creates maps easily, and integrates disparate databases. CorpsMap will provide the National level geospatial view for USACE.

USACE was also the recipient of the first annual OGC Vision Award. This award recognizes the outstanding contribution the USACE has made to the organization and growth of OGC, an international public/private partnership working to make geographic information and services openly accessible across multiple platforms and devices – especially Geospatial SOA.

SOA Development, Test, and Evaluation Lab

For this project a distributed SOA laboratory for Services Development, Test, and Evaluation (DT&E) Laboratory was developed to -

- Reconcile requirements and expertise across organizations.
- Provide a collaborative, distributed, service-oriented build time development environment.
- Demonstrate a secure, shared, service-oriented runtime test environment where prototype capability bundles can be adaptively verified and validated against common government requirements.
- Execute scenarios and document Use Cases for role-based access control.
- Document Best Practices

Using this community SOA space was a natural place to assess enterprise requirements and consistent with PGF SOA guidelines. While testing service performance in this type of federated environment was challenging, the benefits of a common testing capability were substantial. In particular, the DT&E ensured that Best Practices were implementable under near-operational conditions.

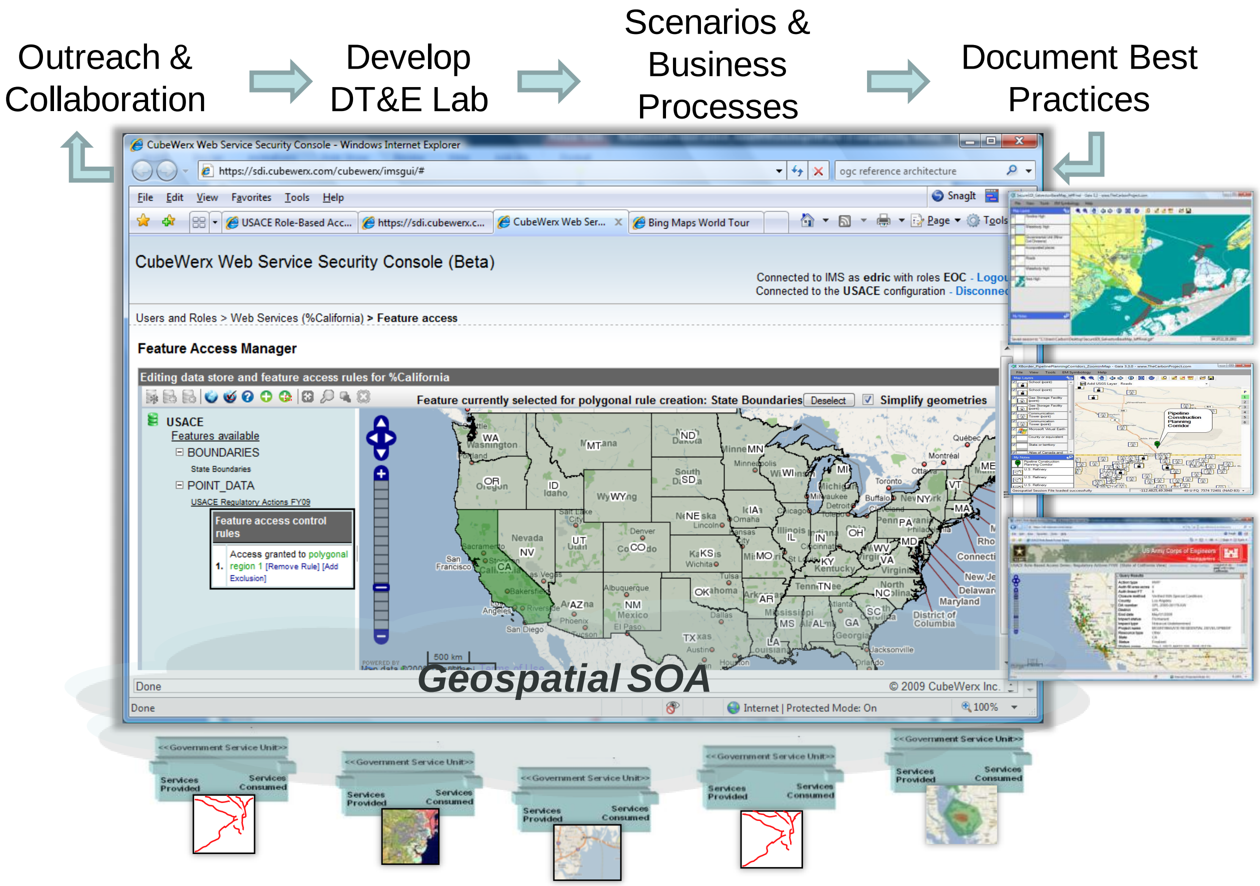

Outreach & Collaboration
Develop DT&E Lab
Scenarios & Business Processes
Document Best Practices
CubeWerx Web Service Security Console - Windows Internet Explorer
https://sdi.cubewerx.com/cubewerx/imsgui/#
CubeWerx Web Service Security Console (Beta)
Connected to IMS as edric with roles EOC - Logout
Connected to the USACE configuration - Disconnect
Users and Roles > Web Services (%California) > Feature access
Feature Access Manager
Editing data store and feature access rules for %California
Feature currently selected for polygonal rule creation: State Boundaries
Deselect
Simplify geometries
USACE
Features available
BOUNDARIES
State Boundaries
POINT_DATA
USACE Regulatory Actions FY09
Feature access control rules
1. Access granted to polygonal region 1 [Remove Rule] [Add Exclusion]
Geospatial SOA
Done
© 2009 CubeWerx Inc.
Internet | Protected Mode: On
100%
<<Government Service Unit>>
Services Provided
Services Consumed

Figure 4 - Distributed SOA laboratory for Services Development, Test, and Evaluation (DT&E) Laboratory

Requirements and Process Definition

In using the DT&E CubeWerx USA followed the general development pattern agreed upon by the three CAP Category 2 awardees: model process and elucidate requirements, design and develop, implement and test, deploy and monitor. The first step has been broken down further into the following components:

1) Document Business Process
2) Create Concept of Operations
3) Develop Detailed Use Cases
4) Generate Technical Requirements

Our requirements gathering phase started during the proposal formulation stage. At that time we assessed specific secure Geospatial SOA, Web services and Web-based applications needs of USACE. After researching Role-based Access Control to meet the operational needs of USACE, we proposed our solution which was met favorably. The proposed test environment for documenting Best Practices for role-based access control in a distributed SOA and collaborative Spatial Data Infrastructure environment were specifically designed to follow a SOA model in a loosely coupled architecture suitable for USACE and other agencies. In response to these requirements CubeWerx USA proposed the implementation of an Identity

Management Service that integrates the Authentication**,** Single Sign-On and Role-based Access Control operations. However, the project adopted the philosophy of using Authentication methods defined by IT industry-wide efforts - and focused on defining simple, reusable *SDI Access Control Rules* for granting access to OGC services by role, geographic extent, feature and SDI operations. The approach is compatible with IT industry-wide efforts working on "Identity Metasystems" to provide an interoperable architecture for digital identity using multiple authentication mechanisms including username and password, x509 certificates, OASIS security standards for Information Cards plus other methods, and the Web Services Protocol Stack that includes WS-Security, WS-Trust, WS-MetadataExchange and WS-SecurityPolicy.

After the project kickoff, CubeWerx USA established an initial the DT&E test environment and a secure version of the NSDI Web Feature Service (WFS) located at http://frameworkwfs.usgs.gov for initial project Use Case and Best Practice development. Initial Use Cases were developed to capture the expected way users will interact with the test service and are split into scenarios describing the steps taken to accomplish a required task, using the system as a tool.

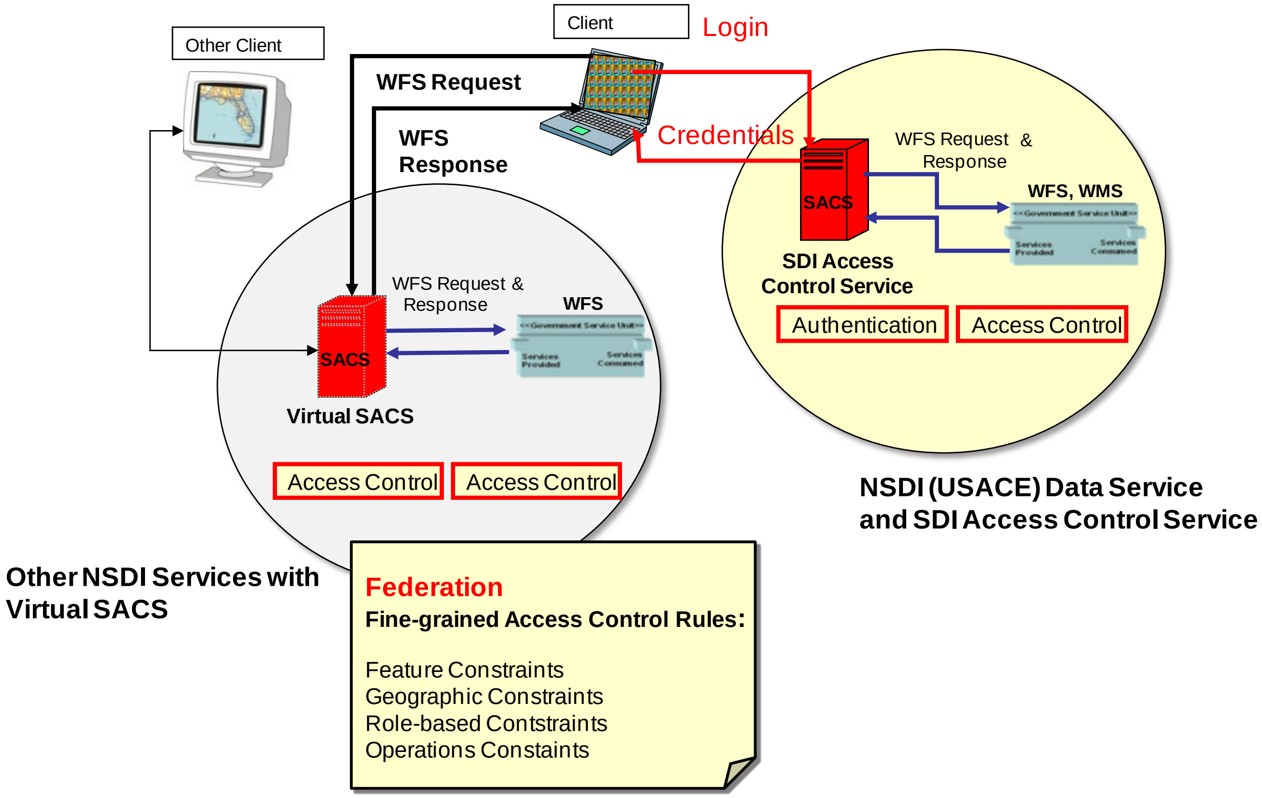


Figure 5 – The basic access control scenario includes a USACE Client accessing resource at USACE. An alternate scenario includes a USACE Client accessing resource at USACE and at other locations in the NSDI

Initial development followed this basic usage scenario and concept of operation:

1. USACE stakeholder equipped with a web based application connects to the Identity Management Server using a valid "username/ password".

2. The Identity Management Server accesses a local authentication service and upon valid authentication returns credentials to the application.
3. Customer application, using the credentials, formulates requests for web resources at a different site.
4. Identity Management Server enforces the customer's credentials, and access control rules.
5. If granted, customer's requests for web resources are processed normally.
6. Fine grain access control rules for OGC WFS Services are enforced by an SDI Access Control Service.
7. NSDI WFS returns appropriate Features.

This scenario is depicted in Figure 5 and highlights the two major deployment situations where data is secured with the USACE enterprise and also leveraged across multiple NSDI enterprises.

Using the DT&E the project began describing the basic system roles, groups and their relationship to access control rules in an NSDI organization. By specifying rules for web services, the SDI Access Control Service can grant unrestricted access to geospatial SOA 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 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 ("*What*"), a rule specifies, for a given set of users ("*Who*"), the conditions under which access is to be granted to them ("*How*"). A user can be associated with **roles** within an organization ("Jeff is a *Portal Manager*") or with a **group** whose membership is known throughout the system (e.g., "Jeff is currently working on *Project Katrina*"). Access control rules at any NSDI organization can refer to these roles (e.g., "*Grant access to any Portal Manager*") and groups (e.g., "*Grant access to any member of Project Katrina*").

Because rules will refer to user roles and names ("*Grant access to Jeff the Portal Manager*"), an SDI Access Control Service 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. The SDI Access Control Service has a flexible authentication framework that supports multiple authentication methods. To authenticate a user known to an organization, IMS uses systems already used to authenticate users. This allows an organization to use existing authentication methods. A user might be authenticated at an organization by providing a username/password that is recognized in the organization, or via X.509 certificates.

Using the initial using the DT&E we reviewed the business processes needed by the US Army Corp of Engineers and began documenting these in a use case format agreed to by the Category 2 project participants. Information gathered provided us sufficient data to develop detailed use cases for system interactions. Specifically, after reviewing several basic scenarios we assessed there are at least five potential system Actors involved in Role-based Access Control Use Cases. These include:

- USACE Data Provider
  A USACE "eGIS" data provider maintains a locally, regionally or nationally bounded vector dataset for their own use and wishes as well to contribute to local, regional or national access.
- NSDI Data Provider
  A data provider not in USACE that maintains a locally, regionally or nationally bounded vector dataset for their own use and wishes as well to contribute to local, regional or national access.
- USACE End User

USACE end users wish to discover, view, and obtain current feature datasets which may cover any part of the United States but which are customized to the user's area of interest.

- NSDI End User
  End users not in USACE that wish to discover, view, and obtain current feature datasets which may cover any part of the United States but which are customized to the user's area of interest.
- USACE Security Manager
  A USACE "eGIS" security manager who grants unrestricted access to geospatial SOA resources to some users, limited kinds of access to other users access.

The project team to then developed and refined 10 Use Cases demonstrating Role-based Access Control defined in Appendix B and summarized in Figure 6. All Actors in these Use Cases must "Login".

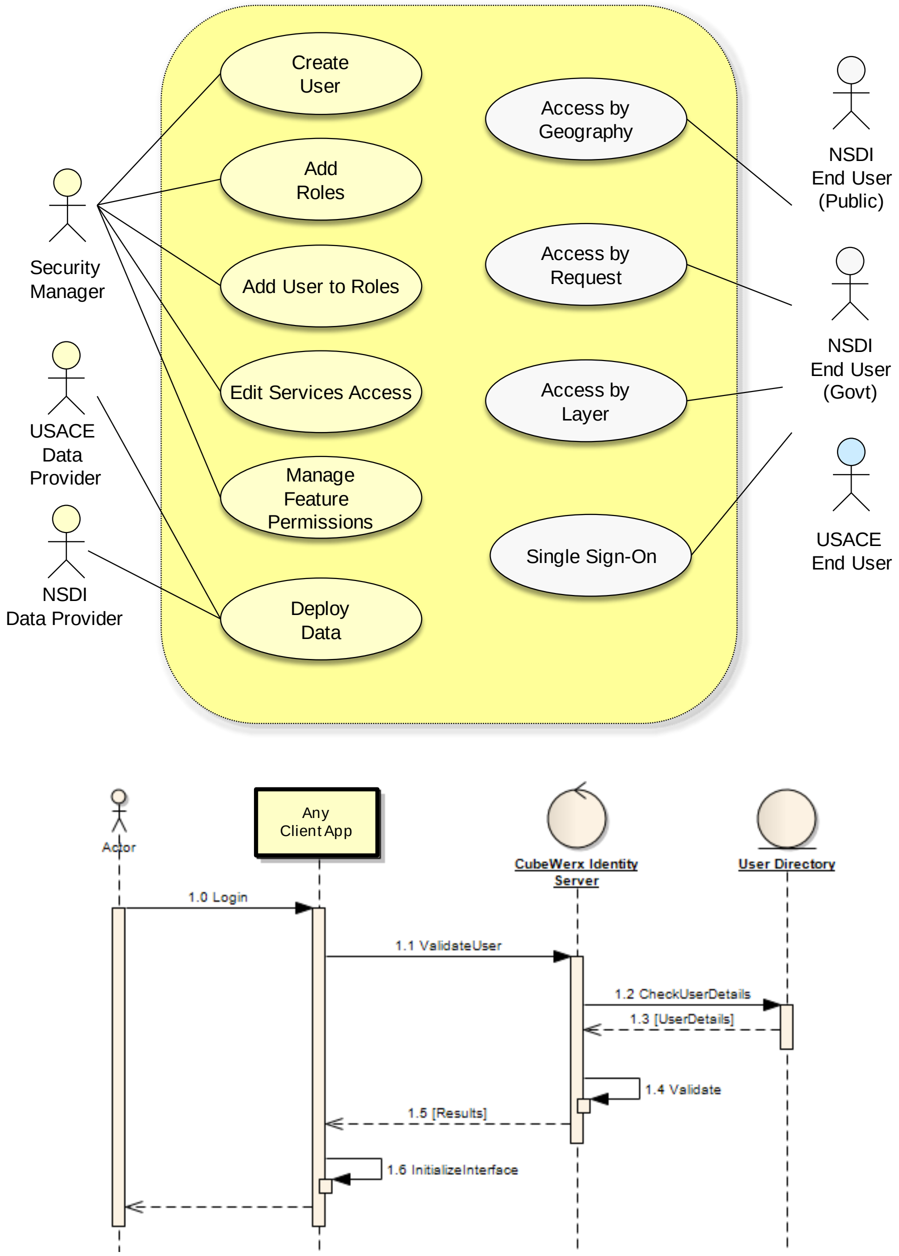


Figure 6 – Role-based Access Control Use Case Diagrams where NSDI 'Provider' Actors are depicted on the left of the IMS system and NSDI 'Consumer' Actors on the right. It is assumed all Actors must "Login" as shown.

SOA Deployment and Acceptance

Using these roles and use cases, the project then established three test scenarios to be executed from October 2008 to mid-2009. These scenarios are described in the following sections, and were documented in various live forums including GEOINT 2008 (October 2008), the FGDC Homeland Security Working Group (January 2009), the HIFLD Working Group (January 2009), the first Geospatial SOA and Cloud Computing Workshop (June 2009) and other venues.

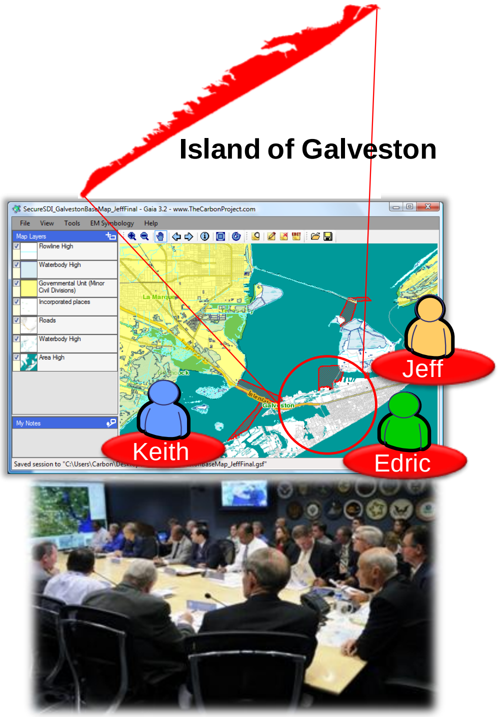
Our effort assessed that these Actors may engage in at least the 10 Use Cases for Role-based Access Control. However, this model needed to be exercised in practice with a variety of data. Accordingly, to further refine the Use Cases, Best Practices and Access Control Rules we developed three test scenarios involving real-world deployment and operations:

- Response to a Hurricane event along the Gulf coast of the United States.
- A Cross-Border SDI project planning event.
- A USACE regulatory permitting business process.

The Capstone scenario for the project deployed actual USACE data and applied all lessons learned to the challenge of providing role-based access to regulatory geospatial data.

Hurricane Response Scenario

The Hurricane response scenario was set on the Gulf Coast of the United States (Figure 7) and included three test Roles – NSDI User – 'Jeff', USACE EOC User – 'Keith', and an NSDI Data Provider – 'Edric.



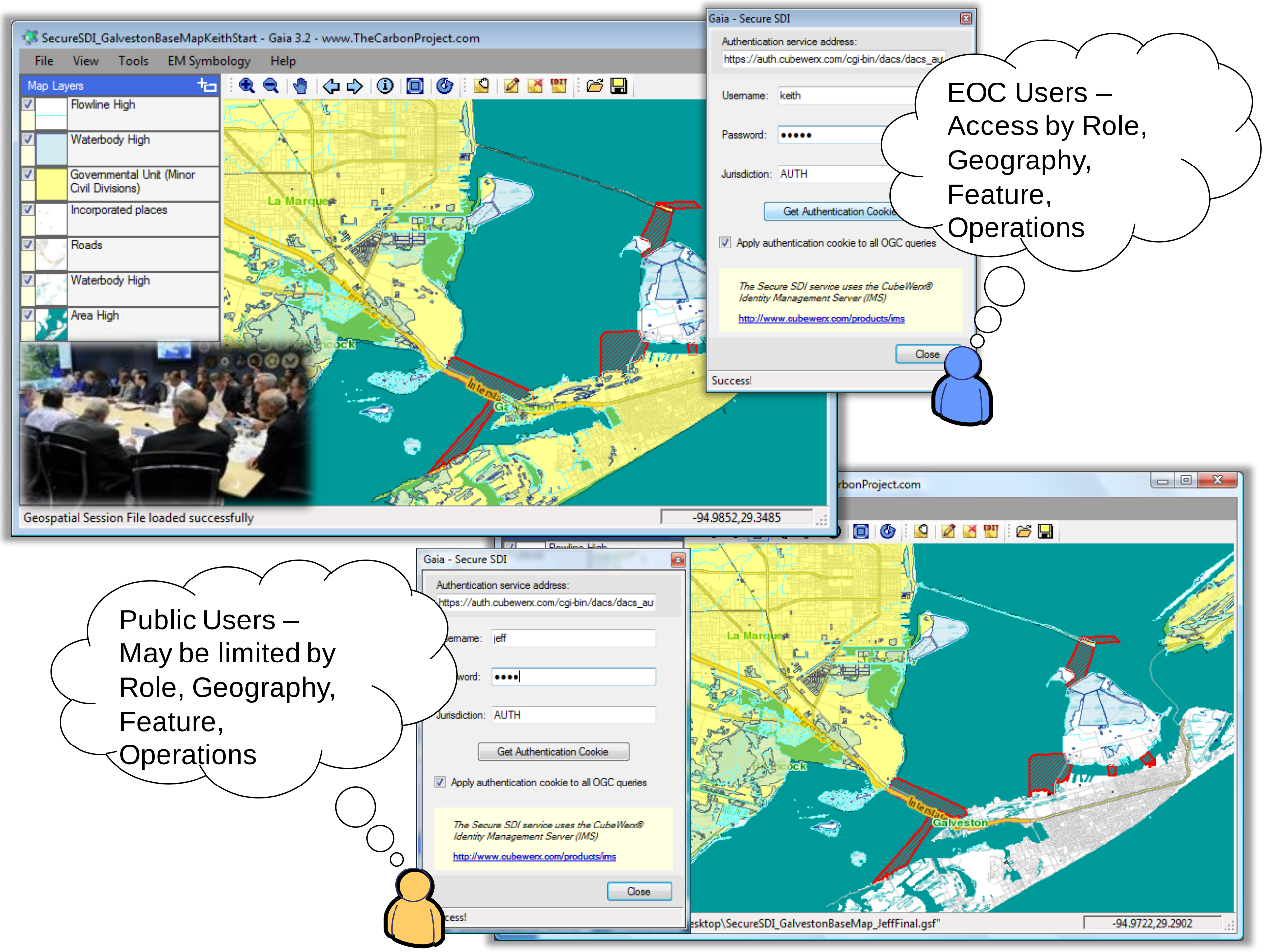
Saved session to "C:\Users\Carbon\Desk…BaseMap_JeffFinal.gsf"

Figure 7 - The Hurricane response scenario was set on the Gulf Coast of the United States and included Public, EOC and NSDI Service Provider Roles

The scenario tested Access Control by *Role, Geography, Feature and OGC Operation* using a modification to the prototype Framework Data Service located at http://frameworkwfs.usgs.gov. To support scenario development and system testing we engaged The Carbon Project[4] to extend its NSDI viewer, Gaia, with a Secure SDI Extension. This extension allowed the project team to test and refine Best Practices assumptions under simulated 'real-world' conditions. An example of Gaia 3.2 implementing Role-based Access Control under simulated conditions is provided in Figure 8 below. This tool is available as a free download from –

http://www.thecarbonportal.net/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=2

The Carbon Project also implemented Secure SDI tools in their extension to ArcGIS 9.2 Desktop, CarbonArc® PRO.[5] This tool allowed advanced functions such as role-based transactions from within ArcGIS, where data update was limited to only authorized Roles.


SecureSDI_GalvestonBaseMapKeithStart - Gaia 3.2 - www.TheCarbonProject.com
File
View
Tools
EM Symbology
Help
Map Layers
Flowline High
Waterbody High
Governmental Unit (Minor Civil Divisions)
Incorporated places
Roads
Waterbody High
Area High
La Marque
Interstate
Galveston
Geospatial Session File loaded successfully
-94.9852,29.3485
rbonProject.com
Flowline High
esktop\SecureSDI_GalvestonBaseMap_JeffFinal.gsf"
-94.9722,29.2902

Gaia - Secure SDI

Authentication service address: https://auth.cubewerx.com/cgi-bin/dacs/dacs_au

Username: keith

Password: •••••

Jurisdiction: AUTH

Get Authentication Cookie

☑ Apply authentication cookie to all OGC queries

The Secure SDI service uses the CubeWerx® Identity Management Server (IMS)

http://www.cubewerx.com/products/ims

Close

Success!

EOC Users – Access by Role, Geography, Feature, Operations

Gaia - Secure SDI

Authentication service address: https://auth.cubewerx.com/cgi-bin/dacs/dacs_au

ername: jeff

word: ••••

Jurisdiction: AUTH

Get Authentication Cookie

☑ Apply authentication cookie to all OGC queries

The Secure SDI service uses the CubeWerx® Identity Management Server (IMS)

http://www.cubewerx.com/products/ims

Close

cess!

Public Users – May be limited by Role, Geography, Feature, Operations

Figure 8 - The hurricane scenario developed test Access Control Rules for limiting access by Role, Geography, OGC Request and Layer

[4] www.thecarbonproject.com

[5] http://www.thecarbonproject.com/carbonarc.php

A key element of the Hurricane Scenario involved the development and modeling of Access Control Rules developed by NSDI Service Providers. By specifying rules for web services, the SDI Access Control Service granted unrestricted access to geospatial SOA resources to the NSDI Service Provider, limited kinds of access to other users such as EOC members, and in some cases completely denied access to yet another set of users. Each access control rule granted (or denied) requests made by an individual or group of individuals, depending on details associated with the request. Referring to a secure version of the NSDI WFS ("*What*"), the rules specifies, for a given set of users ("*Who*"), the conditions under which access is to be granted to them ("*How*"). A user can be associated with **roles** within an organization ("Keith is *an EOC Member*") or with a **group** whose membership is known throughout the system (e.g., " Keith is currently working on *Project Ike*"). Access control rules then referred to these roles (e.g., "*Grant access to any EOC Member*") and groups (e.g., "*Grant access to any member of Project Ike*").

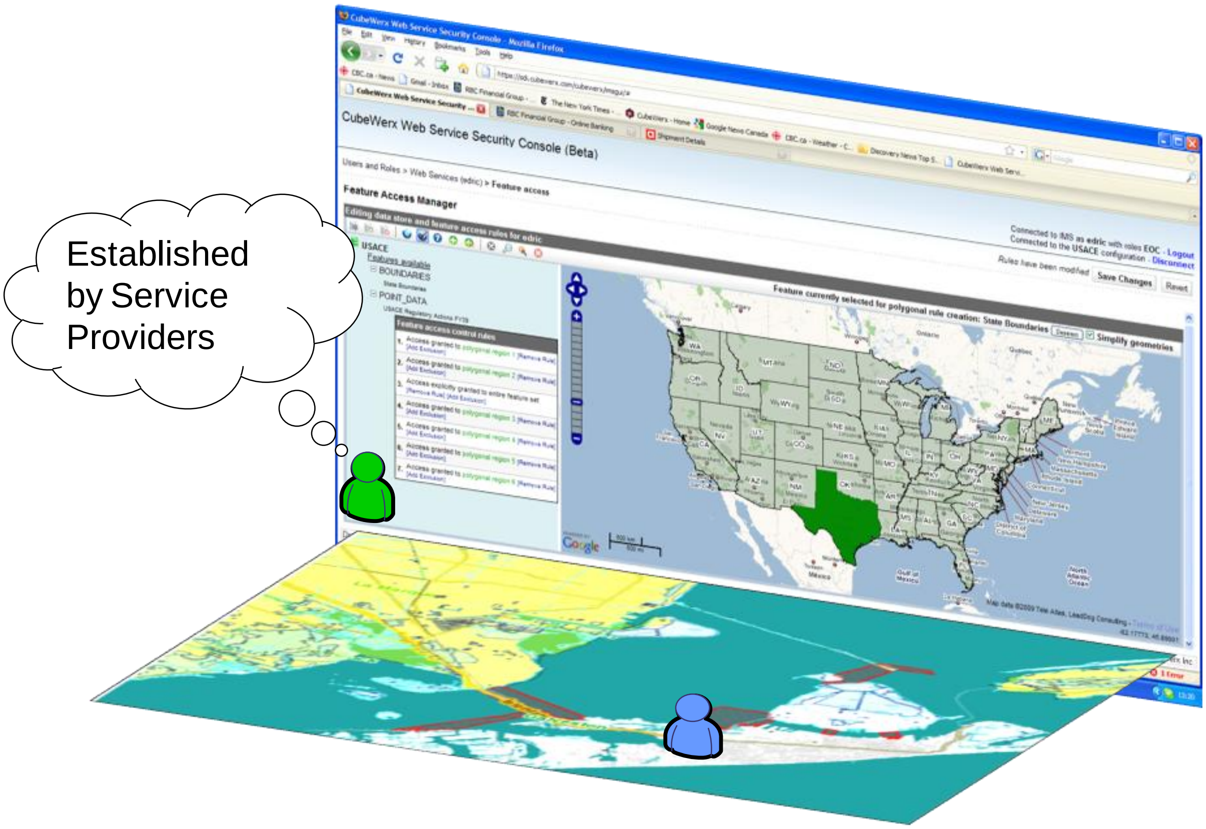

Established by Service Providers
CubeWerx Web Service Security Console (Beta)
Feature Access Manager
Save Changes
Revert

Figure 9 -A key element of the scenario was development of test Access Control Rules

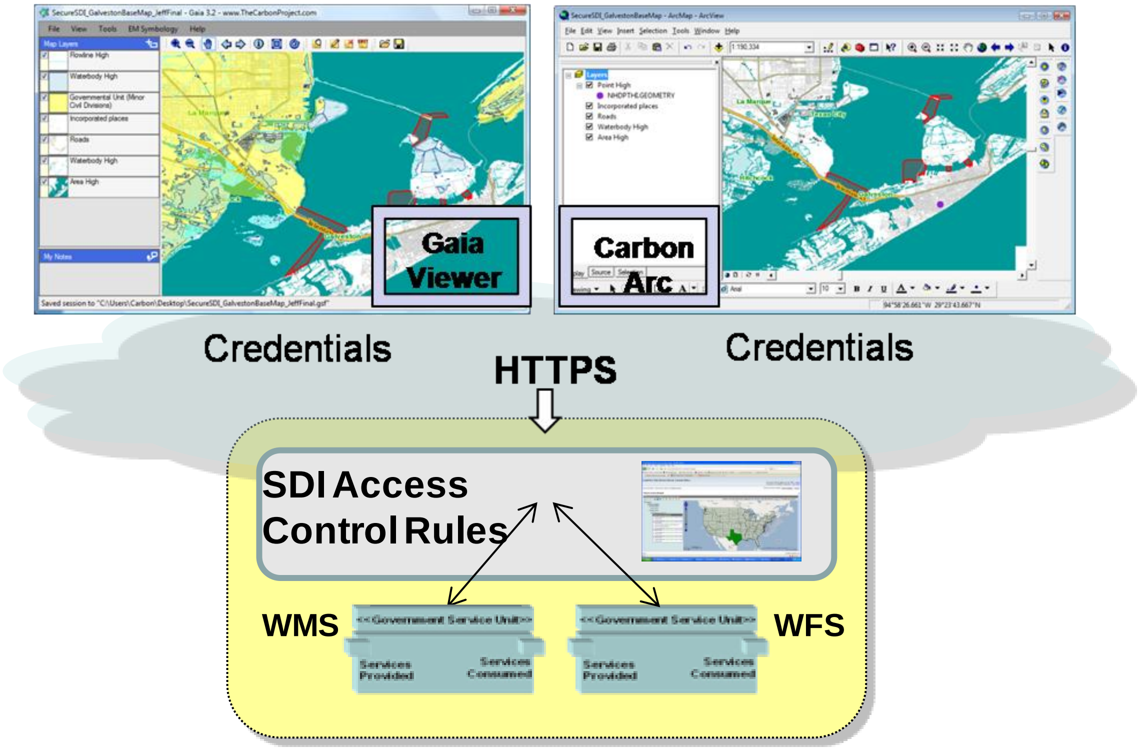


Figure 10 - Architecture of the Hurricane scenario using the Framework WMS and WFS

Cross-Border Pipeline Planning Scenario

At 5,500 miles, the US and Canada share the world's longest common border and identifying critical infrastructures is a vital function for organizations in the cross-border region. With this requirement in mind the Cross-Border SDI Project scenario was set on the border of the United States and Canada, and included two test Roles and focused on Single-Sign-On (Figure 11) –

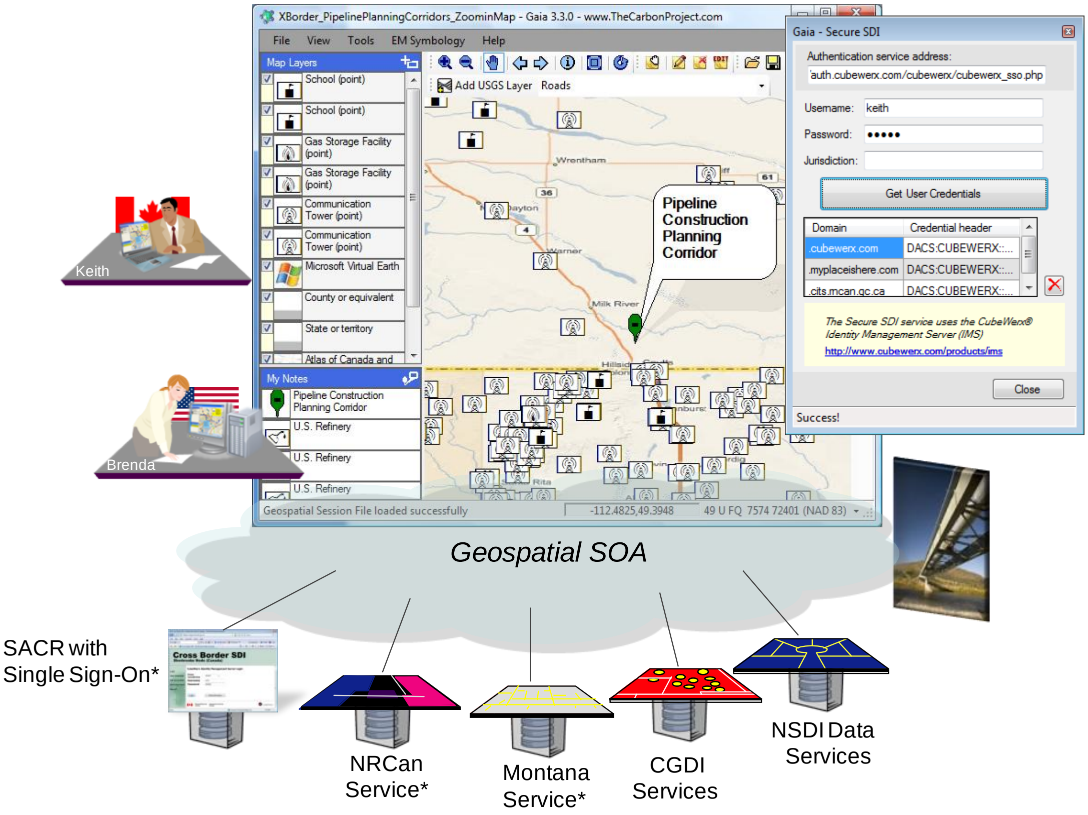
- Planning Commission Engineer in US – 'Brenda'
- Planning Commission Engineer in Canada – 'Keith'

In this scenario an International Planning Commission is reviewing plans for a new oil pipeline. The pipeline is to carry crude oil from western Canada provinces to refineries in US, and the *Planning Corridor* crosses Montana/Saskatchewan border. The Review infrastructure in Planning Corridor & rapidly develop a report. To support scenario development and system testing we used The Carbon Project's Gaia SDI Platform[6] with a Secure SDI Extension and prototype secure Web Feature Services deployed in Montana and Canada.[7]

This scenario also deployed a Web-based application for Single-Sign on using Open Layers (Figure 12). This Cross-Border mashup merges Google Maps, OGC WMS and WFS, Secure SDI and FGDC Emergency Mapping Symbology - and provides an easy way to make sure critical geospatial information goes to the people who are supposed to have it.

[6] http://www.thecarbonproject.com/gaia.php

[7] http://www.thecarbonproject.com/Projects/crossborder.php


XBorder_PipelinePlanningCorridors_ZoominMap - Gaia 3.3.0 - www.TheCarbonProject.com
File
View
Tools
EM Symbology
Help
Map Layers
School (point)
School (point)
Gas Storage Facility (point)
Gas Storage Facility (point)
Communication Tower (point)
Communication Tower (point)
Microsoft Virtual Earth
County or equivalent
State or territory
Atlas of Canada and
My Notes
Pipeline Construction Planning Corridor
U.S. Refinery
U.S. Refinery
U.S. Refinery
Add USGS Layer
Roads
Pipeline Construction Planning Corridor
Wrentham
Warner
Milk River
Geospatial Session File loaded successfully
-112.4825,49.3948
49 U FQ 7574 72401 (NAD 83)
Keith
Brenda
Geospatial SOA
SACR with Single Sign-On*
NRCan Service*
Montana Service*
CGDI Services
NSDI Data Services

Gaia - Secure SDI

Authentication service address: 'auth.cubewerx.com/cubewerx/cubewerx_sso.php

Username: keith

Password: •••••

Jurisdiction:

Get User Credentials

Domain	Credential header
.cubewerx.com	DACS:CUBEWERX::...
.myplaceishere.com	DACS:CUBEWERX::...
.cits.mcan.gc.ca	DACS:CUBEWERX::...

The Secure SDI service uses the CubeWerx® Identity Management Server (IMS)

http://www.cubewerx.com/products/ims

Close

Success!

Figure 11 - The Cross-Border SDI Project scenario was set on the border of the United States and Canada, and included two test Roles focused on Single-Sign-On

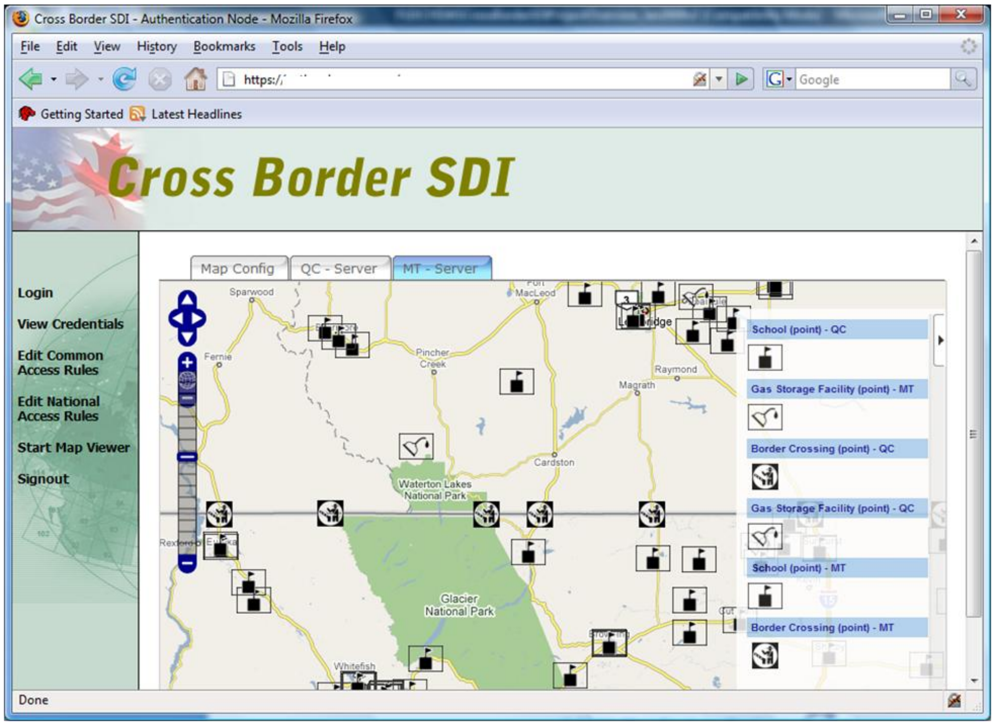


Figure 12 - Cross-Border mashup merges Google Maps, OGC WMS and WFS, Access Control and FGDC Emergency Mapping Symbology

This scenario was demonstrated in multiple public venues and the Single Sign-On sequence using Gaia is available for review online at -

http://carboncloud.blogspot.com/2009/03/cross-border-demo-using-secure-sdi-wfs.html

During this portion of the project we documented the mechanism to provide certificate-based credentials for open geospatial services, including secure Web Feature Services (WFS) to software client applications. From the client perspective there are two key functionalities –

- Logging into an Authentication Service to access the credentials needed.
- Applying these credentials to OGC WFS services to enable response to queries with information according to the user rights and access rules.

The system can be used in a distributed environment which requires any software client to apply corresponding certificates to non-specific ubiquitous servers. To support the Secure SDI system The Carbon Project used the CarbonTools PRO[8] capability to alter the HTTP request at the communications layer, and add new functionality to its Gaia[9] (through an Extender API plug-in) and CarbonArc® PRO[10] products.

To get the required user credentials the client application needs to log-in to a Secure SDI Authentication service. In order to achieve that functionality, The Carbon Project added a tool in the form of a dialog that allows the user to type in a user name and password (Figure 13). The user can also set the authentication service URL and add an optional jurisdiction parameter. Once the information is set clicking on a 'Get User Credentials' button will fetch the list of credentials from the authentication service. This process is done through a simple GET type HTTPS request. For usability purposes the Web call to the authentication service is performed asynchronously.

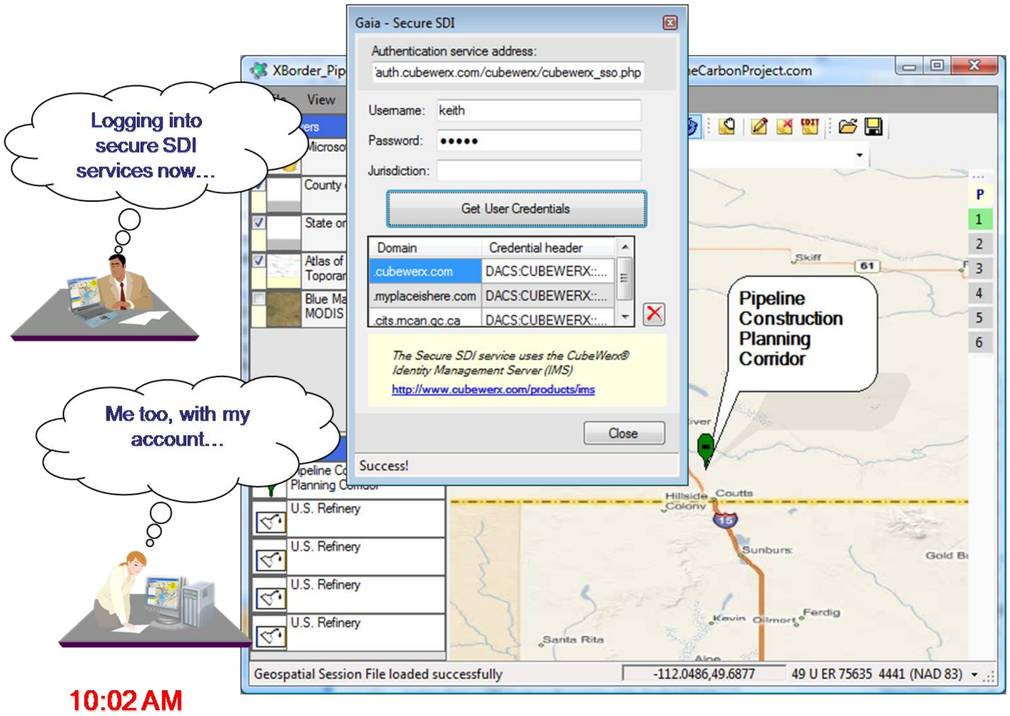
Once the service responds the client analyzes the XML payload and the HTTPS headers. The XML part of the response contains a 'cookie-name' reference. This value allows the client to go through the list of HTTPS headers and collect the ones that are credentials according to their 'cookie-name'. Each credential element contains a domain reference. The client adds the information to the CarbonTools PRO domain-specific headers.

CarbonTools PRO provides the distinct ability to control the HTTPS requests sent to OGC Web Services. This level of control over the communication layer is crucial for the Secure SDI implementation. By managing a global header list with specific domain constraints CarbonTools PRO can decide what headers should be added to the HTTPS request before being sent to the OGC service. Therefore, the certificates gathered by the client will now be considered prior to any Web request. To apply a certificate CarbonTools PRO first compares the target URI and the domain of each certificate. If the domain matches the URI the certificate is used. This process does not affect the query payload in any way.

[8] www.carbontools.com

[9] http://www.thecarbonproject.com/gaia.php

[10] http://www.thecarbonproject.com/carbonarc.php



Gaia - Secure SDI

Authentication service address: 'auth.cubewerx.com/cubewerx/cubewerx_sso.php

Username: keith

Password: •••••

Jurisdiction:

Domain	Credential header
.cubewerx.com	DACS:CUBEWERX:...
.myplaceishere.com	DACS:CUBEWERX:...
.cits.mcan.gc.ca	DACS:CUBEWERX:...

The Secure SDI service uses the CubeWerx® Identity Management Server (IMS)
http://www.cubewerx.com/products/ims

Success!

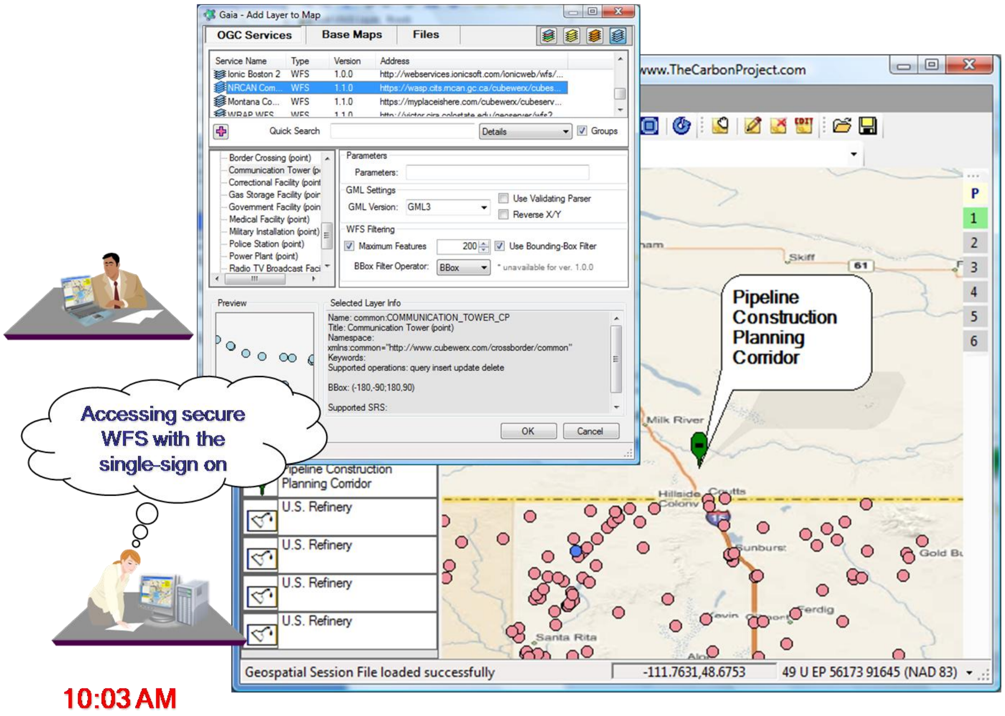
Geospatial Session File loaded successfully

-112.0486,49.6877 49 U ER 75635 4441 (NAD 83)

Figure 13 - To get required user credentials, client applications need to log-in to an Authentication Service

Since the certificates are inspected and applied at the communication layer of CarbonTools PRO all queries are affected (Figure 14). Therefore, getting Service Description (called Capabilities), features or performing transactions on a WFS-T will all use the appropriate certificate. Furthermore, if a user has more than one certificate associated with the service, for example by belonging to more than one authentication group, all credentials will be applied to the query.

In case access is not granted the server returns a ‘Forbidden’ error (403) and a report will be issued on the CarbonTools PRO internal messages log. In Gaia, for example, this will result in the inability to read the service capabilities or perform any updates on data layer coming from the secured service. When access is granted the user can access the service normally, allowing capabilities, features and maps to be read. However, the response will take into account the privileges granted to the certificate holder by the management system.



Gaia - Add Layer to Map

Service Name	Type	Version	Address
Ionic Boston 2	WFS	1.0.0	http://webservices.ionicsoft.com/ionicweb/wfs/...
NRCAN Com...	WFS	1.1.0	https://wasp.cits.rncan.gc.ca/cubewerx/cubes...
Montana Co...	WFS	1.1.0	https://myplaceishere.com/cubewerx/cubeserv...
WRAP WFS	WFS	1.1.0	http://victor.cira.colostate.edu/geoserver/wfs?

Quick Search: Details ☑ Groups

- Border Crossing (point)
- Communication Tower (p
- Correctional Facility (point
- Gas Storage Facility (poir
- Government Facility (poin
- Medical Facility (point)
- Military Installation (point)
- Police Station (point)
- Power Plant (point)
- Radio TV Broadcast Faci

Parameters
Parameters:

GML Settings
GML Version: GML3
□ Use Validating Parser
□ Reverse X/Y

WFS Filtering
☑ Maximum Features 200
☑ Use Bounding-Box Filter
BBox Filter Operator: BBox
* unavailable for ver. 1.0.0

Preview

Selected Layer Info
Name: common:COMMUNICATION_TOWER_CP
Title: Communication Tower (point)
Namespace:
xmlns:common="http://www.cubewerx.com/crossborder/common"
Keywords:
Supported operations: query insert update delete

BBox: (-180,-90;180,90)

Supported SRS:

www.TheCarbonProject.com

Geospatial Session File loaded successfully   -111.7631,48.6753   49 U EP 56173 91645 (NAD 83)

Figure 14 - Once the credentials are acquired they were applied to both the US and Canadian WFS in the security jurisdiction

USACE Regulatory Scenario

The capstone scenario for the project deployed actual USACE data and applied all lessons learned to the challenge of providing role-based access to regulatory geospatial data. Four sub-scenarios were exercised:

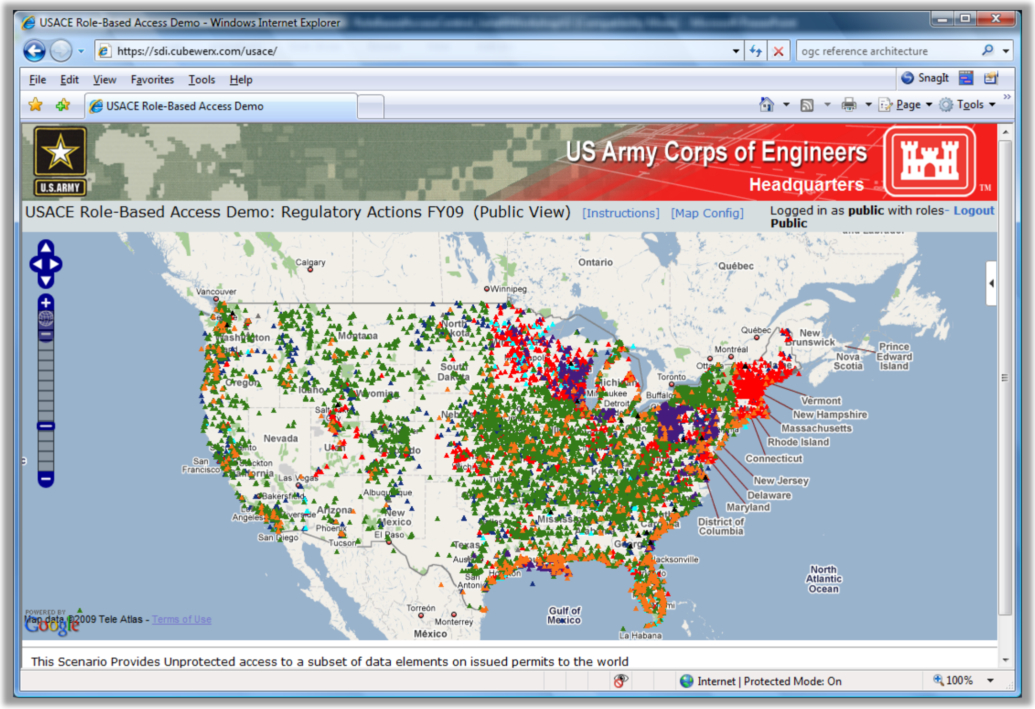
- **Public –** Demonstrates unprotected access to a subset of data elements on issued permits to all users.
- **EPA Region II** - Demonstrates providing jurisdictional information on Pending Actions to EPA Region II.
- **State of California -** Demonstrates authenticated access to consistent view of USACE data in State of California, across 3 USACE districts.
- **USFWS Region IV -** Demonstrates providing permanent wetland impact data to USFWS Region IV.

The demonstrations illustrated role-based access to USACE regulatory data, using four different scenarios, four roles, four users and one simulated Cloud-based Service component deployed as a functional WFS. Each user belongs to one role:

- Public : ‘Public’
- California : ‘Paul’
- EPA Region II : ‘John’
- USFWS Region IV : ‘George’

Each role's access control rules demonstrates a different spatial and non-spatial filter developed according to input provided by USACE. The map configuration for this scenario used Google Maps from the background and secure CubeWerx WMS and WFS for regulatory data overlays.

The Public Scenario illustrated open access to a subset of data elements on issued permits (Figure 15). The ‘California’ Scenario demonstrates providing authenticated access to a consistent view of USACE data for the State of California with data across multiple USACE districts (Figure 16). The ‘EPA Region 2’ scenario demonstrates providing Jurisdictional information on Pending Actions to EPA Region II (Figure 17). The USFWS Region IV Scenario demos providing permanent wetland impact data to USFWS Region IV (Figure 18).



USACE Role-Based Access Demo - Windows Internet Explorer

https://sdi.cubewerx.com/usace/

ogc reference architecture

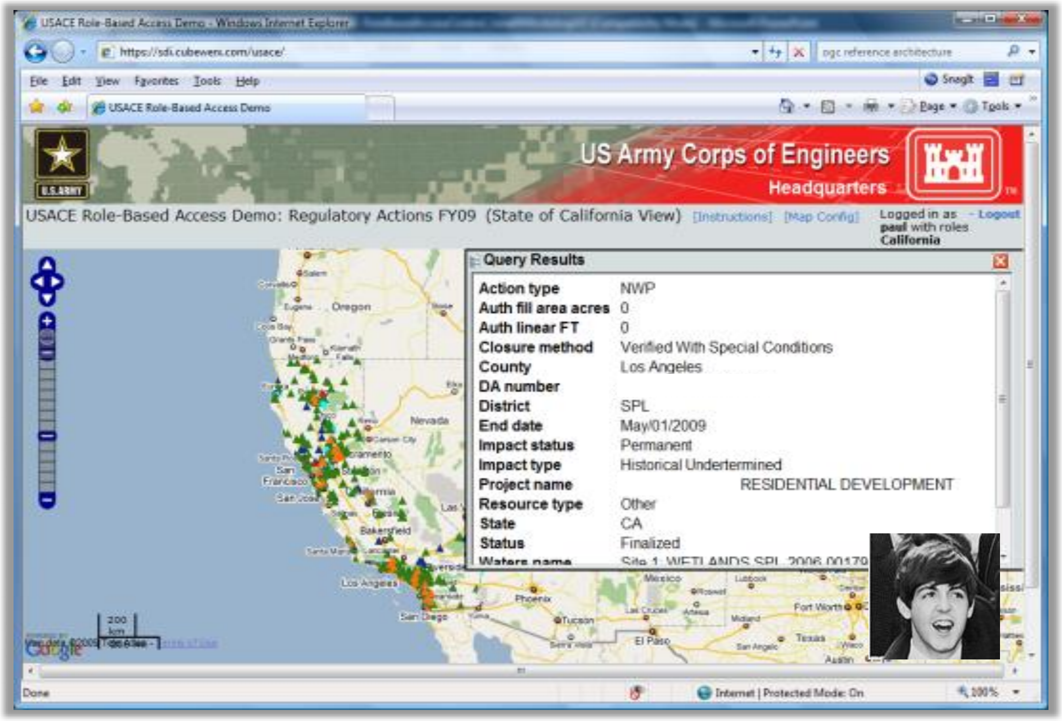
USACE Role-Based Access Demo: Regulatory Actions FY09 (Public View) [Instructions] [Map Config]

Logged in as **public** with roles- **Logout**
Public

This Scenario Provides Unprotected access to a subset of data elements on issued permits to the world

Internet | Protected Mode: On

Figure 15 - Public Scenario, open access to a subset of data elements on issued permits

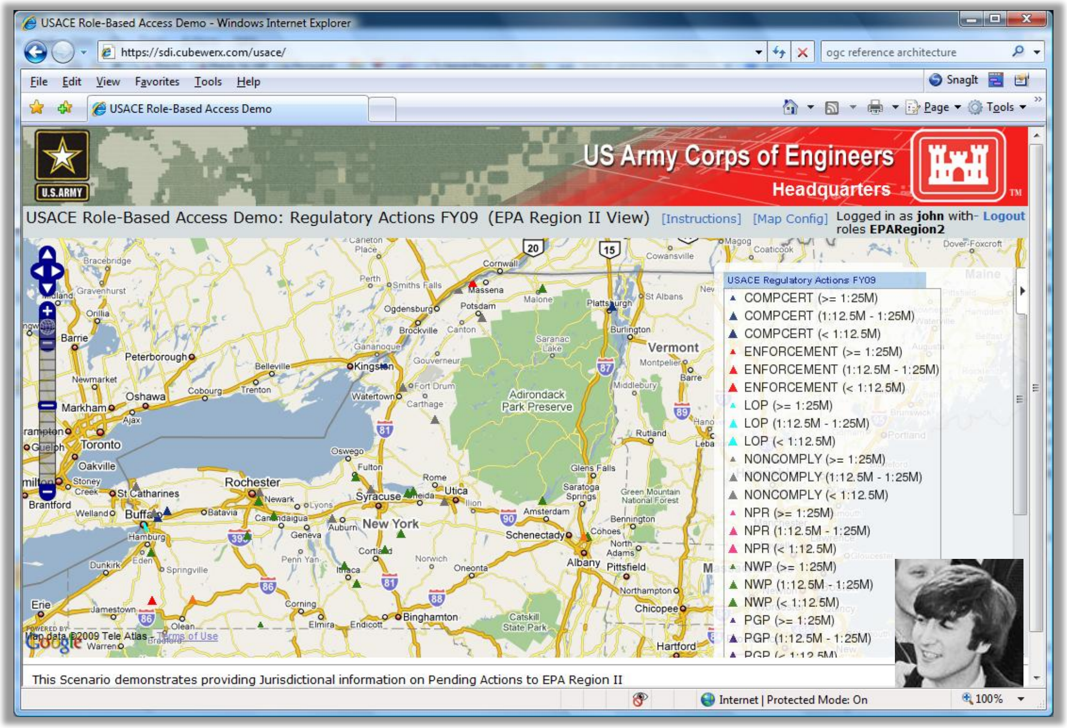

USACE Role-Based Access Demo - Windows Internet Explorer
https://sdi.cubewerx.com/usace/
ogc reference architecture
File Edit View Favorites Tools Help
Snagit
USACE Role-Based Access Demo
Page Tools
U.S.ARMY
US Army Corps of Engineers
Headquarters
Oregon
Nevada
San Francisco
San Jose
Bakersfield
Los Angeles
San Diego
Phoenix
Tucson
El Paso
Texas
Fort Worth
200 km
Done
Internet | Protected Mode: On
100%

USACE Role-Based Access Demo: Regulatory Actions FY09 (State of California View) [Instructions] [Map Config] Logged in as paul with roles California - Logout

Query Results

Action type	NWP
Auth fill area acres	0
Auth linear FT	0
Closure method	Verified With Special Conditions
County	Los Angeles
DA number	
District	SPL
End date	May/01/2009
Impact status	Permanent
Impact type	Historical Undertermined
Project name	RESIDENTIAL DEVELOPMENT
Resource type	Other
State	CA
Status	Finalized
Waters name	Site 1: WETLANDS SPL 2006 00179

Figure 16 - 'California' Scenario demonstrates providing authenticated access to a consistent view of USACE data for the State of California


USACE Role-Based Access Demo - Windows Internet Explorer
https://sdi.cubewerx.com/usace/
ogc reference architecture
File Edit View Favorites Tools Help
Snagit
USACE Role-Based Access Demo
Page Tools
U.S.ARMY
US Army Corps of Engineers
Headquarters
Toronto
Rochester
Buffalo
Syracuse
New York
Utica
Albany
Schenectady
Binghamton
Kingston
Vermont
Adirondack Park Preserve
Hartford
Internet | Protected Mode: On
100%

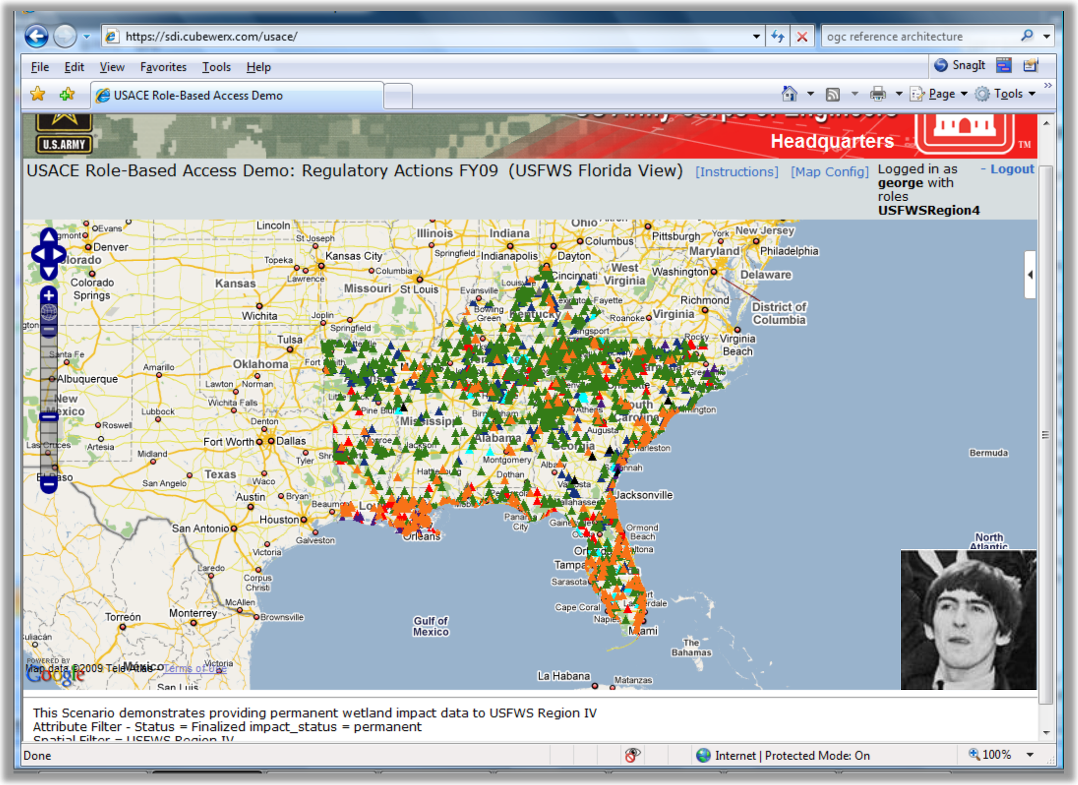
USACE Role-Based Access Demo: Regulatory Actions FY09 (EPA Region II View) [Instructions] [Map Config] Logged in as john with roles EPARegion2 - Logout

USACE Regulatory Actions FY09

- ▲ COMPCERT (>= 1:25M)
- ▲ COMPCERT (1:12.5M - 1:25M)
- ▲ COMPCERT (< 1:12.5M)
- ▲ ENFORCEMENT (>= 1:25M)
- ▲ ENFORCEMENT (1:12.5M - 1:25M)
- ▲ ENFORCEMENT (< 1:12.5M)
- ▲ LOP (>= 1:25M)
- ▲ LOP (1:12.5M - 1:25M)
- ▲ LOP (< 1:12.5M)
- ▲ NONCOMPLY (>= 1:25M)
- ▲ NONCOMPLY (1:12.5M - 1:25M)
- ▲ NONCOMPLY (< 1:12.5M)
- ▲ NPR (>= 1:25M)
- ▲ NPR (1:12.5M - 1:25M)
- ▲ NPR (< 1:12.5M)
- ▲ NWP (>= 1:25M)
- ▲ NWP (1:12.5M - 1:25M)
- ▲ NWP (< 1:12.5M)
- ▲ PGP (>= 1:25M)
- ▲ PGP (1:12.5M - 1:25M)
- ▲ PGP (< 1:12.5M)

This Scenario demonstrates providing Jurisdictional information on Pending Actions to EPA Region II

Figure 17 - EPA Region 2' scenario demonstrates providing Jurisdictional information on Pending Actions to EPA Region II



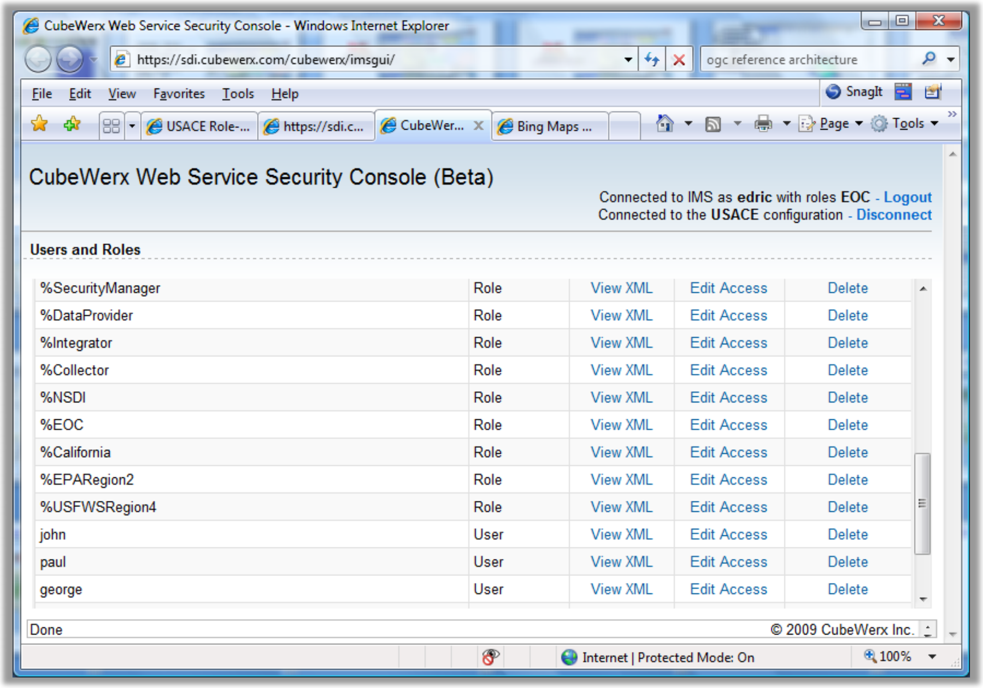
USACE Role-Based Access Demo: Regulatory Actions FY09 (USFWS Florida View)

Logged in as **george** with roles **USFWSRegion4**

This Scenario demonstrates providing permanent wetland impact data to USFWS Region IV
Attribute Filter - Status = Finalized impact_status = permanent
Spatial Filter = USFWS Region IV

Figure 18 – Final scenario demos providing permanent wetland impact data to USFWS Region IV

A key element of the regulatory scenario was the use of actual USACE permitting data to develop Access Control Rules to model real-world deployment challenges (Figures 17-19).



CubeWerx Web Service Security Console (Beta)

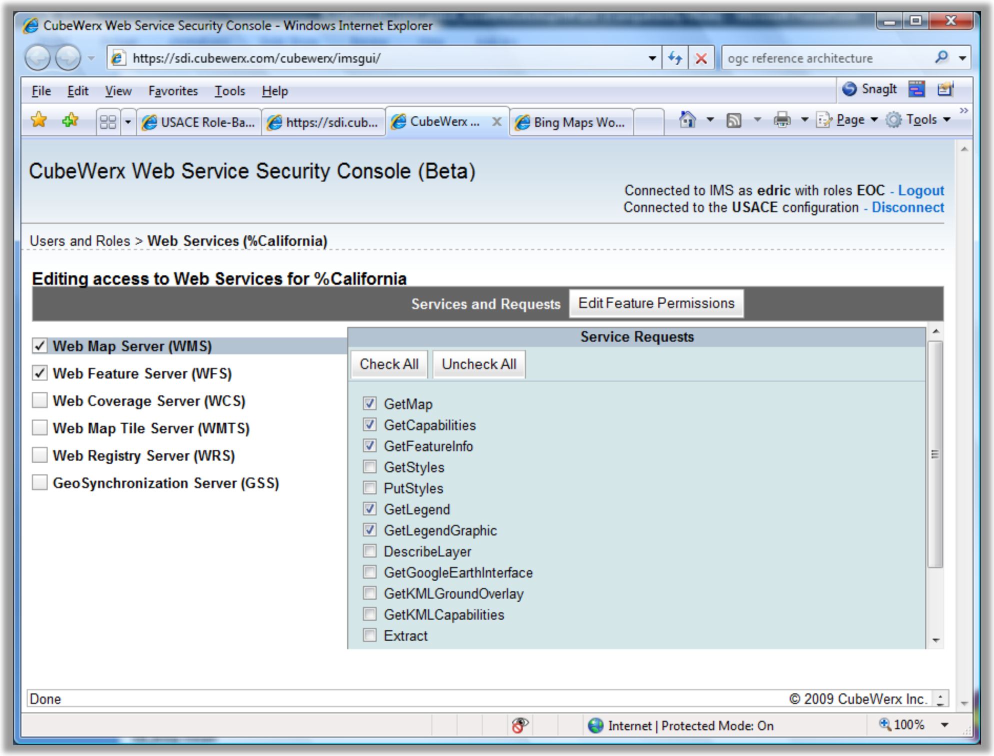
Connected to IMS as **edric** with roles **EOC** - Logout
Connected to the **USACE** configuration - Disconnect

Users and Roles

%SecurityManager	Role	View XML	Edit Access	Delete
%DataProvider	Role	View XML	Edit Access	Delete
%Integrator	Role	View XML	Edit Access	Delete
%Collector	Role	View XML	Edit Access	Delete
%NSDI	Role	View XML	Edit Access	Delete
%EOC	Role	View XML	Edit Access	Delete
%California	Role	View XML	Edit Access	Delete
%EPARegion2	Role	View XML	Edit Access	Delete
%USFWSRegion4	Role	View XML	Edit Access	Delete
john	User	View XML	Edit Access	Delete
paul	User	View XML	Edit Access	Delete
george	User	View XML	Edit Access	Delete

CubeWerx Web Service Security Console - Windows Internet Explorer
https://sdi.cubewerx.com/cubewerx/imsgui/
ogc reference architecture
File Edit View Favorites Tools Help
SnagIt
USACE Role-...
https://sdi.c...
CubeWer...
Bing Maps ...
Page
Tools
Done
© 2009 CubeWerx Inc.
Internet | Protected Mode: On
100%

Figure 19 – Development of Roles for Regulatory Permitting



CubeWerx Web Service Security Console (Beta)

Connected to IMS as **edric** with roles **EOC** - Logout
Connected to the **USACE** configuration - Disconnect

Users and Roles > **Web Services (%California)**

Editing access to Web Services for %California

Services and Requests | Edit Feature Permissions

☑ Web Map Server (WMS)
☑ Web Feature Server (WFS)
☐ Web Coverage Server (WCS)
☐ Web Map Tile Server (WMTS)
☐ Web Registry Server (WRS)
☐ GeoSynchronization Server (GSS)

Service Requests

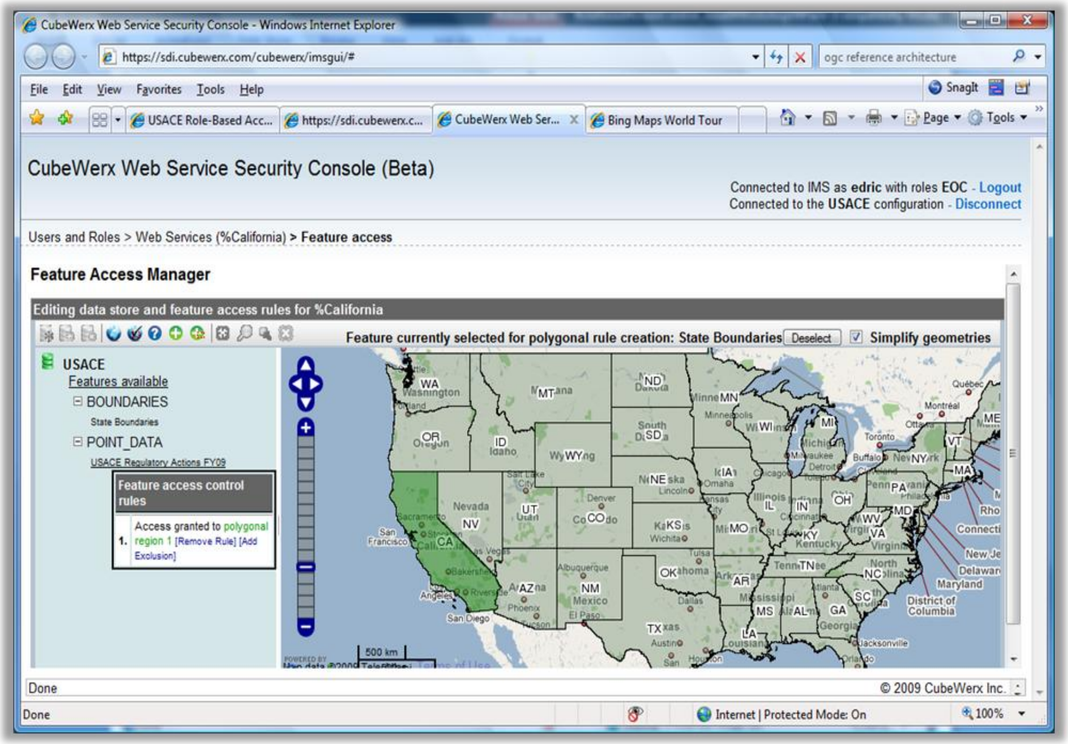
Check All | Uncheck All

☑ GetMap
☑ GetCapabilities
☑ GetFeatureInfo
☐ GetStyles
☐ PutStyles
☑ GetLegend
☑ GetLegendGraphic
☐ DescribeLayer
☐ GetGoogleEarthInterface
☐ GetKMLGroundOverlay
☐ GetKMLCapabilities
☐ Extract

CubeWerx Web Service Security Console - Windows Internet Explorer
https://sdi.cubewerx.com/cubewerx/imsgui/
ogc reference architecture
File Edit View Favorites Tools Help
SnagIt
USACE Role-Ba...
https://sdi.cub...
CubeWerx ...
Bing Maps Wo...
Page
Tools
Done
© 2009 CubeWerx Inc.
Internet | Protected Mode: On
100%

Figure 20 – Establishing Access to Web Services for Regulatory Permitting

For example, the USGS framework data GML polygon for 'California' was used to develop an ACR to enable just the appropriate data to be deployed to the correct users (Figure 20).


CubeWerx Web Service Security Console (Beta)

Connected to IMS as **edric** with roles **EOC** - Logout
Connected to the **USACE** configuration - Disconnect

Users and Roles > Web Services (%California) > **Feature access**

Feature Access Manager

Editing data store and feature access rules for %California

Feature currently selected for polygonal rule creation: State Boundaries Deselect ☑ Simplify geometries

USACE
Features available
⊟ BOUNDARIES
State Boundaries
⊟ POINT_DATA
USACE Regulatory Actions FY09

Feature access control rules

1. Access granted to polygonal region 1 [Remove Rule] [Add Exclusion]

CubeWerx Web Service Security Console - Windows Internet Explorer
https://sdi.cubewerx.com/cubewerx/imsgui/#
ogc reference architecture
File Edit View Favorites Tools Help
SnagIt
USACE Role-Based Acc...
https://sdi.cubewerx.c...
CubeWerx Web Ser...
Bing Maps World Tour
Page
Tools
WA
MT
ND
MN
OR
ID
SD
WY
WI
MI
NY
VT
ME
MA
NE
IA
PA
OH
IN
IL
NV
UT
CO
CA
KS
MO
KY
WV
VA
MD
AZ
NM
OK
AR
TN
NC
SC
MS
AL
GA
TX
LA
500 km
Done
© 2009 CubeWerx Inc.
Internet | Protected Mode: On
100%

Figure 21 - USGS framework data GML polygon for ‘California’ used to develop an ACR

Best Practices - Access Control Rules for OGC Services

This section describes the structure of the Access Control Rules developed and deployed by CubeWerx during this project. These Access Control Rules have been defined through an XML Schema using an XML file that can be dynamically parsed by an OGC compliant Government Service Unit such as a Web Feature Service (WFS) or Web Map Service (WMS).

As presented in the Access Control XML Schema below, the contents of the root <AccessControlRules> element are zero or more <Rule> elements, each having a mandatory appliesTo attribute. Unless an Authentication server product is being used, only one <Rule> element with appliesTo="everybody" needs to exist. As indicated by the attribute value, this rule applies to all users.

The <Rule> element contains one or more <AllowedRequests> and <AllowedLayers> elements. When only a single rule is present, each of these elements should be present at least once. An <AllowedRequests> element specifies which requests should be made available for the service specified by the service attribute (where * means “all”). It consists of a series of <Allow> and <Exclude> elements, each containing the name of a request (where * means “all”). The set of allowed requests for the specified service is the union of the requests itemized by the <Allow> elements minus the union of the requests itemized by the <Exclude> elements.

Similarly, the <AllowedLayers> element specifies which layers should be made available for the named data store specified by the dataStore attribute (where * means “all”). It consists of a series of <Allow> and <Exclude> elements, each containing the name of a layer (where * means “all”). The set of allowed layers is the union of the layers itemized by the <Allow> elements minus the union of the layers itemized by the <Exclude> elements.

An example will help clarify the use of an Access Control rule XML file. XML document:

```
<AccessControlRules>
<Rule appliesTo="everybody">
<AllowedRequests service="WMS">
<Allow>*</Allow>
<Exclude>PutStyles</Exclude>
<Exclude>Extract</Exclude>
</AllowedRequests>
<AllowedRequests service="WFS">
<Allow>GetCapabilities</Allow>
<Allow>DescribeFeatureType</Allow>
<Allow>GetFeature</Allow>
</AllowedRequests>
...
<AllowedLayers dataStore="*">
<Allow>*</Allow>
</AllowedLayers>
</Rule>
</AccessControlRules>
```

These rules state that all users have access to every WMS request except for PutStyles and Extract, and also have access to the three specific WFS requests GetCapabilities, DescribeFeatureType and GetFeature. Access to every layer in every data store listed in the dataStores (or activeDataStores) configuration parameter is granted. It should be noted that Rules explicitly grant access. No rule explicitly restricts access. So a complete absence of rules indicates that no access is permitted. Each rule created explicitly grants access to users or group of users.

The base elements of the rule file are *Rule* elements. *Rule* elements contain an attribute indicating who the rule applies to, using a set of one or more *AllowedRequests* and *AllowedLayers* elements. *AllowedRequests* elements refer to OGC Web Service Requests. The Service type (WFS, WMS etc) is specified as an attribute of the *AllowedRequests* element. *AllowedLayers* elements specify which layers (or features) in the service the user indicated by the rule may have access to. Both the *AllowedRequests* and *AllowedLayers* elements contain *Allow* and *Exclude* elements. What each rule allows is the union of its *Allow* elements minus the union of its *Exclude* elements. *Allow* and *Exclude* elements in *AllowedLayers* may have an optional area syntax, indicating a geographical area that the Allow applies to.

The full Rule file schema is provided below:

```
<schema
  targetNamespace="http://schemas.cubewerx.com/namespaces/accessControl"
  xmlns="http://www.w3.org/2001/XMLSchema"
```

```
 xmlns:accessControl="http://schemas.cubewerx.com/namespaces/accessControl"
 elementFormDefault="qualified"
 version="0.0.2">

<element name="AccessControlRules">
  <complexType>
    <sequence>
      <element ref="accessControl:Rule"
              minOccurs="0" maxOccurs="unbounded"/>
    </sequence>
  </complexType>
</element>

<element name="Rule">
  <complexType>
    <choice minOccurs="0" maxOccurs="unbounded">
      <element ref="accessControl:AllowedRequests"/>
      <element ref="accessControl:AllowedLayers"/>
    </choice>
    <!-- The "appliesTo" attribute is a comma-separated list of        -->
    <!-- username, groups and roles that this rule applies to.         -->
    <!-- Usernames are of the form "[<jurisdiction>:]<user>", and      -->
    <!-- groups and roles are of the form "%[<jurisdiction>:]<group>". -->
    <!-- In both cases, either or both of jurisdiction and user/group  -->
    <!-- can be "*", meaning "all" (or the jurisdiction name and colon -->
    <!-- can be left out completely).  Three special usernames exist:  -->
    <!-- "[<jurisdiction>:]auth", meaning any authorized user of the   -->
    <!-- specified jurisdiction, "unauth", meaning any user who is     -->
    <!-- not authorized at all, and "everybody", which matches all     -->
    <!-- users.  Note that "everybody" is NOT the same as "*:*", but   -->
    <!-- IS the same as "auth,unauth".                                 -->

    <!-- Unless the CubeWerx Identity Management Server product -->
    <!-- is in use, the only valid value for this attribute is  -->
    <!-- "everybody".                                           -->

    <!-- More than one rule can apply at any given time.  In    -->
    <!-- this situation, access is granted to the union of what -->
    <!-- is granted by each of the applicable rule.             -->
    <attribute name="appliesTo" type="string" use="required"/>
  </complexType>
</element>

<element name="AllowedRequests">
  <!-- The set of requests that this element grants access to    -->
  <!-- for the specified service (where "*" means all) is equal  -->
  <!-- to the union of the requests itemized by the <Allow>      -->
  <!-- elements minus the union of the requests itemized by the  -->
  <!-- <Exclude> elements.  Each <Allow> and <Exclude> element   -->
  <!-- specifies the name of a request (where "*" means "all").  -->
  <complexType>
   <choice minOccurs="0" maxOccurs="unbounded">
    <element name="Allow" type="string"/>
    <element name="Exclude" type="string"/>
   </choice>
  </complexType>
  <attribute name="service" type="string"/>
 </element>

 <element name="AllowedLayers">
  <!-- The set of layers (and areas) within the specified named  -->
  <!-- data store (where "*" means all) that this element grants -->
  <!-- access to is equal to the union of the layers (and areas) -->
  <!-- itemized by the <Allow> elements minus the union of the   -->
  <!-- layers (and areas) itemized by the <Exclude> elements.    -->
  <!--                                                         -->
  <!-- The values of <Allow> and <Exclude> are of the form       -->
  <!-- "<layerName>[<area>]" where rawLayerName can be "*"       -->
  <!-- meaning "all".  If no area is specified, then the entire  -->
  <!-- layer is allowed or excluded.                             -->
  <!-- An area is specified with the following syntax:           -->
  <!-- "{<x1>,<y1>,<x2>,<y2>,...[,<coordinateSystem>]}".         -->
  <!-- If only two pairs of coordinates are given, then the      -->
  <!-- coordinates are interpreted as being the two opposing     -->
  <!-- corners of a box.  If more than two pairs of coordinates  -->
  <!-- are given, then the coordinates are interpreted as being  -->
  <!-- the points of a polygon.  If the coordinate system is     -->
  <!-- omitted, WGS84 Geographic is assumed.                     -->

  <!-- E.g.:                                                     -->
  <!-- <AllowedLayers dataStore="Foundation">                    -->
  <!--   <Allow>GTOPO30{-110,25,-100,40,EPSG:4326}</Allow>       -->
  <!-- </AllowedLayers>                                          -->

  <complexType>
   <choice minOccurs="0" maxOccurs="unbounded">
    <element name="Allow" type="string"/>
    <element name="Exclude" type="string"/>
   </choice>
  </complexType>
  <attribute name="dataStore" type="string"/>
 </element>

</schema>
```

Best Practices - Access Control Rules with Authentication Service

If an Authentication service product is being used, access control can be defined on a user-by-user basis. Digital credentials with zero or more authenticated usernames, groups and roles identifying the current user can be used. Several rules can be specified in an <AccessControlRules> document, where each rule can apply to a different set of usernames, groups and/or roles. The appliesTo attribute of a rule is a comma-separated list of username, groups and/or roles that the rule applies to. Usernames can be of the form [*jurisdiction*:]*user*, and groups and roles are of the form %[*jurisdiction*:]*group*. In both cases, either or both of jurisdiction and user/group can be *, meaning “all” (or the jurisdiction name and colon can be left out completely). Three special usernames would typically exists in such architecture: [*jurisdiction*:]auth, meaning any authorized user of the specified jurisdiction, unauth, meaning any user who is not authorized at all, and everybody, which matches all users. Note that everybody is *not* the same as *:*, but *is* the same as auth,unauth.

A user may match more than one rule. For example, if a user is authenticated as CW:bob which is part of the group %CW:mygroup, then all rules that include CW:bob, %CW:mygroup, CW:*,auth or everybody in the appliesTo list will be active. A user has access to the union of the things that his or her matching rules grant. It is important to note that a rule can only grant access; it can never restrict access. In the absence of a matching rule granting specific access, the default is to deny all access.

The following example illustrates the use of fine-grain access control rules in an environment using an Authentication service:

```
<AccessControlRules>
<!-- Every user, whether authenticated through CubeWerx IMS or -->
<!-- not, has access to the basic WMS operations and a -->
<!-- foundation data set. -->
<Rule appliesTo="everybody">
<AllowedRequests service="WMS">
<Allow>GetCapabilities</Allow>
<Allow>GetMap</Allow>
<Allow>GetFeatureInfo</Allow>
<Allow>GetLegendGraphic</Allow>
</AllowedRequests>
<AllowedLayers dataStore="Foundation">
<Allow>*</Allow>
</AllowedLayers>
</Rule>

<!-- Any user that has been authenticated through CubeWerx IMS -->
<!-- also has access to the WMS Extract operation and -->
<!-- the VMAP Level 1 data set. -->
<Rule appliesTo="auth">
<AllowedRequests service="WMS">
<Allow>Extract</Allow>
</AllowedRequests>
```

```
<AllowedLayers dataStore="Vmap1">
<Allow>*</Allow>
</AllowedLayers>
</Rule>

<!-- Users CW:jim and CW:bob work with satellite data, -->
<!-- so they’re also granted access to all layers of the -->
<!-- Satellite data store, with the exception of the -->
<!-- 1meter ortho layer. -->
<Rule appliesTo="CW:jim,CW:bob">
<AllowedLayers dataStore="Satellite">
<Allow>*</Allow>
<Exclude>1meter ortho</Exclude>
</AllowedLayers>
</Rule>

<!-- User CW:frank is granted access to the WMS GetStyles -->
<!-- and PutStyles operations. -->
<Rule appliesTo="CW:frank">
<AllowedRequests service="WMS">
<Allow>GetStyles</Allow>
<Allow>PutStyles</Allow>
</AllowedRequests>
</Rule>

<!-- Any user that has been authenticated with an CubeWerx IMS -->
<!-- username that is in the %CW:admin group has access -->
<!-- to everything. -->
<Rule appliesTo="%CW:admin">
<AllowedRequests service="*">
<Allow>*</Allow>
</AllowedRequests>
<AllowedLayers dataStore="*">
<Allow>*</Allow>
</AllowedLayers>
</Rule>
</AccessControlRules>
```

In the Access Control rule XML file presented above, every user, whether authenticated through The Access Control Framework or not, is granted access to the basic WMS operations and a foundation data set. No other rule can override this basic access (because, remember, a rule can only grant access; it can never restrict access). If the user is authenticated through The Access Control Framework as being user CW:bob, then that user also has access to the WMS Extract request and the VMAP Level 1 data set (because of the auth rule), as well as most of the Satellite data store (because of the CW:jim,CW:bob rule). If this user is also authenticated as a user who is in the %CW:admin group, then he has access to everything.

The <Exclude> line in the CW:jim,CW:bob rule does *not* mean that he is denied access to the 1meter ortho layer, only that that particular rule does not specifically grant access to it.

Best Practices - Access Control Rules based on Geographic Areas

In addition to being able to grant access to specific layers, it is also possible to grant access to specific *areas*. The full syntax of the <Allow> and <Exclude> elements of the <AllowedLayers> element in an <AccessControlRules> XML document is *layerName*[*area*], where *layerName* can be *, meaning "all". If no area is specified, then the entire layer is allowed or excluded. An area is specified with the following syntax: *{x1,y1,x2,y2*,...[,*coordinateSystem*]*}*. If only two pairs of coordinates are given, then the coordinates are interpreted as being the two opposing corners of a box. If more than two pairs of coordinates are given, then the coordinates are interpreted as being the points of a polygon. If the coordinate system is omitted, WGS84 Geographic is assumed.

For example,

```
<Allow>GTOPO30{-110,25,-100,40,EPSG:4326}</Allow>
```

grants access to the area of the GTOPO30 layer that lies within the WGS84 Geographic box with the corners -110,25 and -100,40. Similarly,

```
<Allow>GTOPO30</Allow>
<Exclude>GTOPO30{-110,25,-100,40,EPSG:4326}</Exclude>
```

grants access to all of GTOPO30 with the exception of the area that lies within the WGS84 Geographic box with the corners -110,25 and -100,40. For a more complicated example, consider the following set of access control rules:

```
<AccessControlRules>
<Rule appliesTo="everybody">
<AllowedRequests service="WMS">
<Allow>*</Allow>
</AllowedRequests>
<AllowedLayers dataStore="Foundation">
<Allow>*{0,4,8,12,EPSG:4326}</Allow>
<Exclude>*{3,0,3,10,13,0,EPSG:4326}</Exclude>
</AllowedLayers>
</Rule>
<Rule appliesTo="everybody">
<AllowedLayers dataStore="Foundation">
<Allow>*{5,2,10,7,EPSG:4326}</Allow>
</AllowedLayers>
</Rule>
</AccessControlRules>
```

It should be noted that the SACR schema used in this project is a simple, functional subset of XACML/geoXACML - but specifically focused on the requirements of OGC SDI (WMS, WFS, WCS, GSS, CS-W, etc.). The project team believes it may be very beneficial for this type of simple Access Control Rules encodings to advance for the NSDI.

Best Practices - User-centric Access Control and Authentication

This Access Control project evaluated a framework that responds to today's "Transacting Web" also named Web 2.0 and addresses security concerned and access control issues related to accessing OGC data services in a distributed and access controlled environment. Simply presented, access control comprises an authentication process – the means by which a user establishes its identity, and an authorization process – the means by which a system determines whether access to a resource should be granted to the user. Under Web 1.0 authentication, these processes were dictated by each site; the concept of identity was site-centric. Under Web 2.0, identities are user-centric. User-centric digital identities, like a driver's license or passport are portable and it is expected that they will be widely recognized and used for supporting privacy requirements over the Web in the years to come. Supporting such standardized digital identities is a shift from ad hoc application-centric authorization mechanisms to user-centric and organization-driven authorization. Web 2.0 applications are also leveraging common, external authorization services managed by identity provider organizations.

A practical design of this technology cannot be based on a centralized system to which all participants are subordinate. A technology architecture for such collaborative systems must provide a framework allowing participating organizations to recognize multiple authentication methods, multiple authorization organizations, and portable standardized digital identities held by users in peer organizations that can be used to grant access to their data resources based on those identities and associated roles. It must be possible to quickly define and re-define access control rules on-the-fly either to widen or further remove access already granted as needed during an emergency situation or for any other requirements.

Until now, authentication processes have been dictated by each Web service provider forcing each user to register and provide personal information at each service provider site prior to receiving access to a service provider site. Currently, the most commonly used authentication method exercised by our software applications is the "user name/ password" method. Major security problems associated to such weak authentication mechanism has forced the software industry at large to react and developed new Web 2.0 security specifications. Standards organizations such as OASIS along with many large private organizations have paved the way with standards such as WS-Security.

But the large majority of our current security implementations are still site-centric. CubeWerx team believes that there is sufficient technology momentum in the IT Industry and capacity available that indicates that authentication processes are shifting to a user-centric mechanism supported by Web 2.0 technology. Like a passport or a driver's license this new digital identity has shifted from ad-hoc application-centric authorization mechanisms and moved to user-controlled and organization-centric authorization mechanisms. Within an SDI environment, a practical design and implementation of a user-centric authentication mechanism has to be based on a security metasystem that provides secured access to Web resources operated in a collaborative and distributed environment.

During this project, The Carbon project and CubeWerx have explored and deployed user-centric Access Control and Authentication services. The Authentication approach modeled in this project is compatible with IT industry-wide efforts working on "Identity Metasystems" to provide an interoperable architecture for digital identity using multiple authentication mechanisms including username and password, x509 certificates, OASIS security standards for Information Cards, and the Web Services Protocol Stack that includes WS-Security, WS-Trust, WS-MetadataExchange and WS-SecurityPolicy (Figure 23). In particular, this *Best Practice for Role-based Access Control* adopted the philosophy of using Authentication methods defined by IT industry-wide efforts and focused on defining simple, reusable *SDI Access Control Rules* for granting access to OGC services by role, geographic extent, feature and SDI operations. This approach adds significant new capability for deploying service components by allowing organizations to optimize data services and reduce costs.

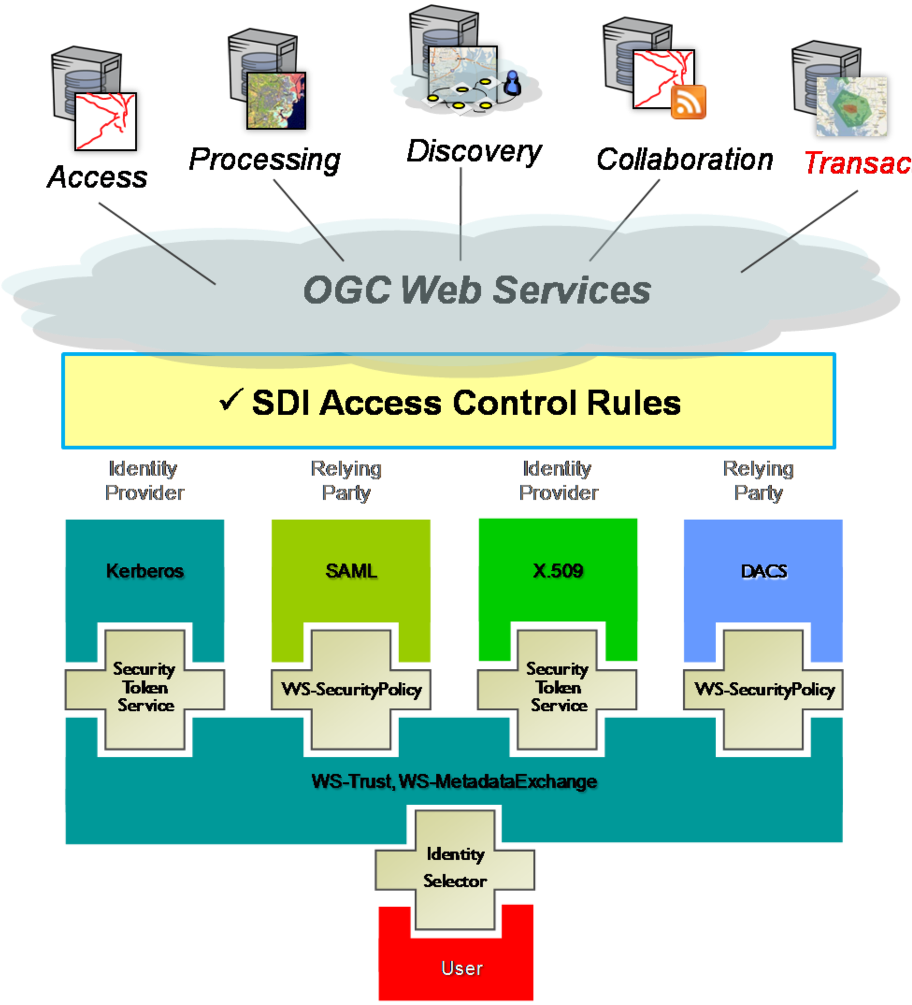


Figure 23 - The Authentication approach modeled in this project is compatible with IT industry-wide efforts

Best Practices - Access Control Rules at Government Service Unit Level

Besides the needs to respond to security concerns associated with allowing access to geospatial data based on digital identities, CubeWerx developed technology to support dynamic access control rules to data services operating in a secured and non-secured distributed geospatial SOA. In many application domains, requirements for geospatial services can change rapidly. For example, during the regulatory permitting process it is not efficient to create a second and third database and deploy a subset of a master database directed at a specific group of people or individuals (Figure 24). In addition, such approaches always result into extra costs for hardware, software and maintenance. A cost effective solution to this problem is to implement access control rules capability allowing data and service administrators to dynamically, over the Web, establish access control rules for their users and group of users when required.

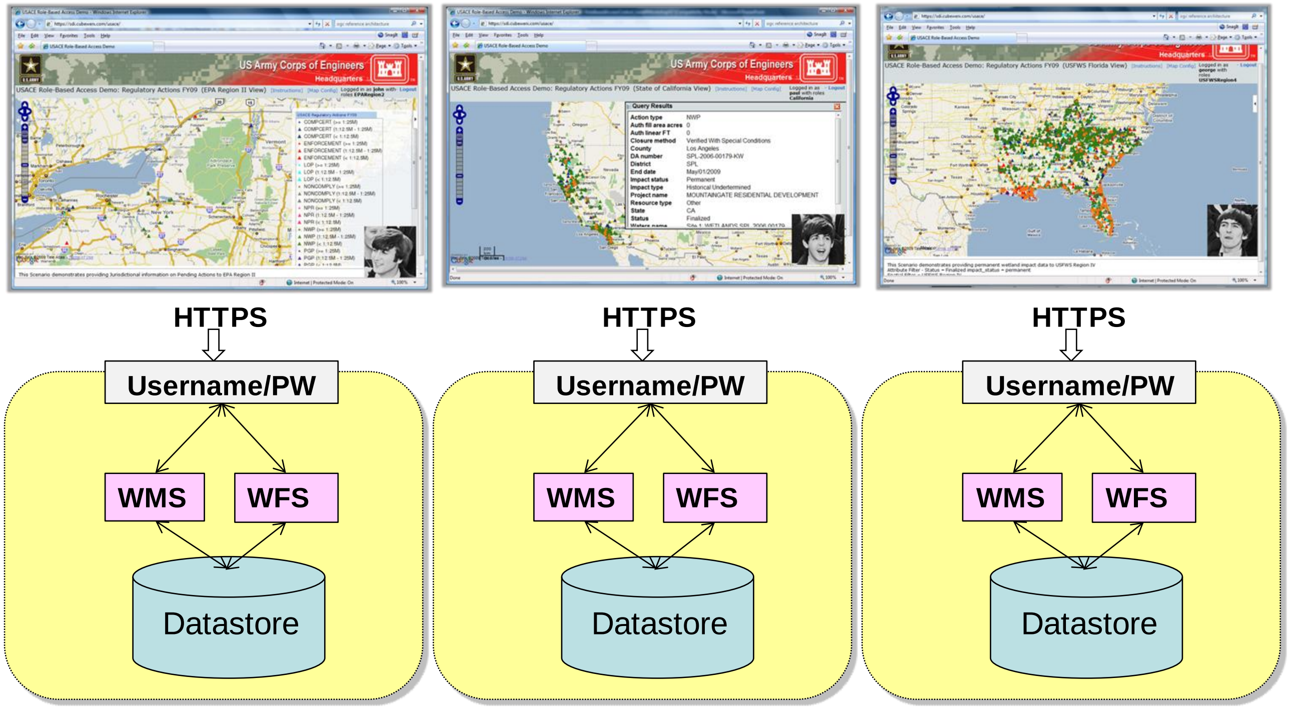


Figure 24 - During the regulatory permitting process it is not efficient to create a second and third database and deploy a subset of a master database directed at a specific group of people or individuals.

The following scenario for Access Control and Authentication illustrates those challenges:

A regulatory organization has a number of geospatial datasets related to emergency situations. An officer of this organization needs to share certain geospatial datasets with other organizations having different access privileges. The officer would like to distribute geospatial data from his OGC compliant Web services and allow his collaborators to easily and efficiently access his data so that he can:

- Share completed permits with specific federal organizations.
- Share with a specific individual at an office, certain permitting features for a specific region (a subset of a complete dataset).
- Grant temporary access to a military official to update pending data layers for a specific region.

The Access Control Rules-based Best Practices in this project improves decision making processes based on Geospatial data by essentially delivering an Access Control and Authentication service that can support secured and controlled access to OGC services using a single regulatory database (Figure 25). This service can be deployed for delivering OGC services in many application domains and in particular with applications operating in real-time environment as described by the scenario above. This project effectively promotes the use of secured SDI Web services within communities of practice through multi-vendor interoperable software products and open standards. This approach is in line with the OGC vision and will further contribute to a growing SDI market by sending a clear message inviting service providers to deploy their secure OGC services using the same OGC compliant architecture and the role they wish to play within the infrastructure. A successful SDI is an infrastructure that is simple and allows anyone to participate or connect.

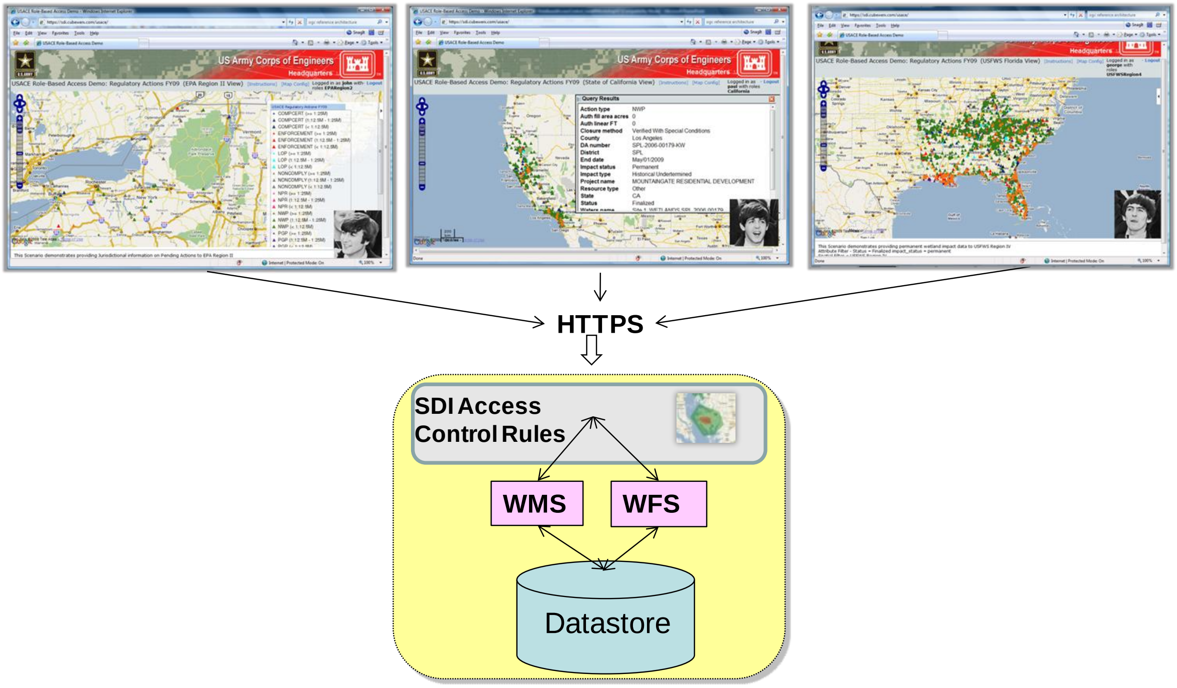


Figure 25 - An Access Control service can support secured and controlled access to OGC services for multiple Roles using a single regulatory database

Best Practices – Reuse of OGC Service Requests for Access Control

A key advantage of the approach tested in this project is that the OGC Services Request framework, an international set of standards, may be reused for the *AllowedRequests* element of the draft schema. This approach enables significant potential savings in SOA design, development and deployment. Specific *AllowedRequests* elements for a Government Service Unit include:

Government Service Unit WMS=>Web Map Server

GetMap
GetCapabilities
GetFeatureInfo

```
GetStyles
PutStyles
GetLegend
GetLegendGraphic
DescribeLayer

Government Service Unit WFS=>Web Feature Server
-----------------------
GetCapabilities
DescribeFeatureType
GetFeature
GetFeatureWithLock
LockFeature
GetGMLObject
Transaction

Government Service Unit WCS=>Web Coverage Server
------------------------
GetCapabilities
DescribeCoverage
GetCoverage

Government Service Unit WMTS=>Web Map Tile Server
-------------------------
GetCapabilities
GetTile
GetAlternateSources

Government Service Unit WRS=>Web Registry Server
------------------------
GetCapabilities
DescribeRecord
GetDomain
GetRecords
GetRecordById
Harvest
UnHarvest
Transaction
GetRecordsSimple
GetRecordsBasic
GetAssociation
ClassifyRecord
GetRepositoryItem
GetWSDL
```

Project Management

It is likely that this project will continue in some form, given the interest expressed in Role-based Access Control. In particular, information from this project will be advanced to the OGC to help develop a simple-to-implement Best Practice for OGC Web Services that is based on Access Control Rules leveraging the established Service Requests suite of widely adopted OGC Web Services such as WMS, WFS, WCS etc. This effort will be coordinated to profile standards such as GeoXACML .

Follow-on phases may consider focused deployment of Access Controlled NSDI Resources in a Cloud-computing environment. The deployed final SOA is suitable for implementation on an EC2 Virtual Machine (provided by Amazon). This type of deployment will allow evaluation of performance characteristics of the service using the following multiple configurations. The focus of such an effort would be to assess scalability, robustness, and overall performance and costs of the service in the cloud environment.

Feedback on Cooperative Agreements Program

The NSDI Cooperative Agreements Program provided an opportunity for CubeWerx researchers to work with NSDI practitioners from USACE and other organizations on an initiative that has real world implications in much of the U.S NSDI. The program provides for the injection of new technologies and approaches into the geospatial community. The grant provided both research challenges and important collaboration experiences.

Strengths: The program reviews and funding decisions were made very quickly. We were also pleased to have the opportunity to prototype services and simulate deployment scenarios with the Cross-Border SDI project and USACE, an effort that came out of discussions and regular teleconferences with the CAP government team. The program's mixture of government, enterprise, and academic teams was also very beneficial. Overall, the program is making very good progress towards promoting key aspects of realizing NSDI services online. Continued emphasis needs to be placed on promoting an online infrastructure of standards-based location content across the nation that can flexibly support operational requirements, and governance of resulting standards for information sharing and security. With the progress on access control exemplified by efforts such as those outlined in this report we can identify no technical impediments to advancing such an infrastructure. However, we suspect funding issues are holding back development of this online infrastructure.

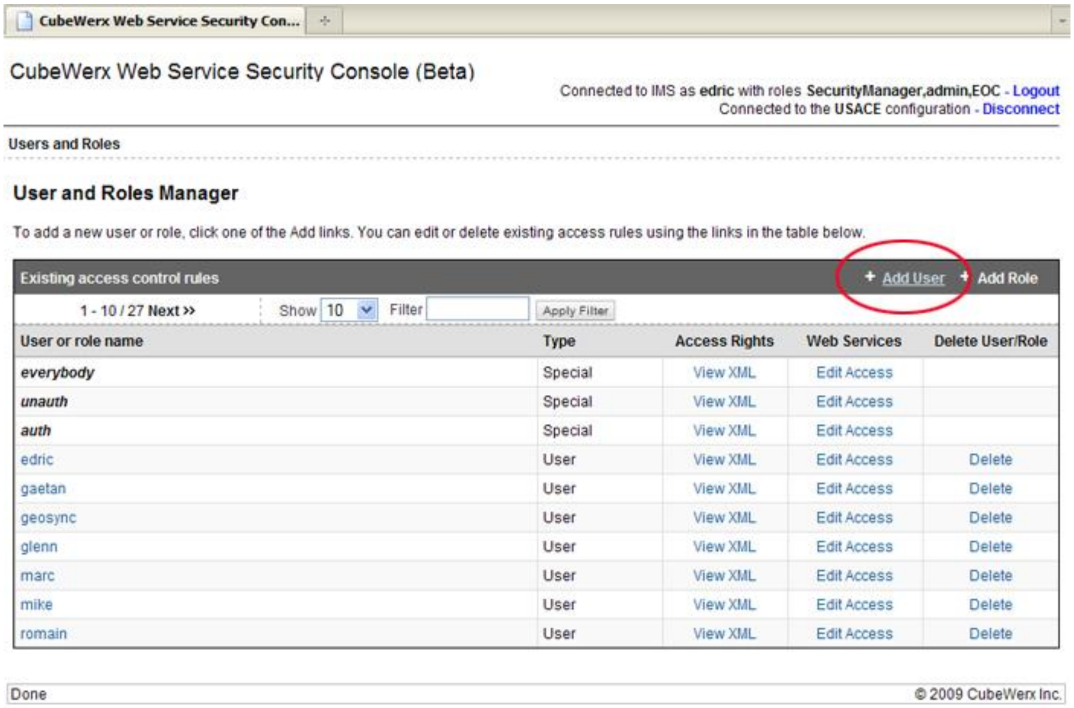
Weaknesses: Although not a weakness, additional external Federal engagement (i.e. outside FGDC) in project continuation and partnering efforts should continue to be encouraged. This is occurring but agencies such as DHS and others can benefit from CAP solutions and should continue to engage more in the process. Specifically, the CAP needs to have continued strong liaison in operational aspects of these agencies and with other state, federal, and commercial interests.

The team had no program management concerns. The team received prompt responses to questions. Additionally the program management team’s format for meetings and communications facilitated collaborations.

Appendix A – Use Cases for Role-based Access Control

Use Case 1 – Create User

Name of use-case	**Create Users**
Actors	Security Manager
Description	An NSDI Security Manager handles NSDI End Users
Pre-conditions	- A secure NSDI or USACE service exists. - NSDI End Users require role-based access.
Flow of events	- Security Manager connects to Web Service Security Console (console starts by default in the User and Roles manager) - Manager clicks Add User, bringing up a dialog where they enter the new user name and password, clicks OK
Post-conditions	- A User is created



CubeWerx Web Service Security Console (Beta)

Connected to IMS as **edric** with roles **SecurityManager,admin,EOC** - Logout
Connected to the **USACE** configuration - Disconnect

Users and Roles

User and Roles Manager

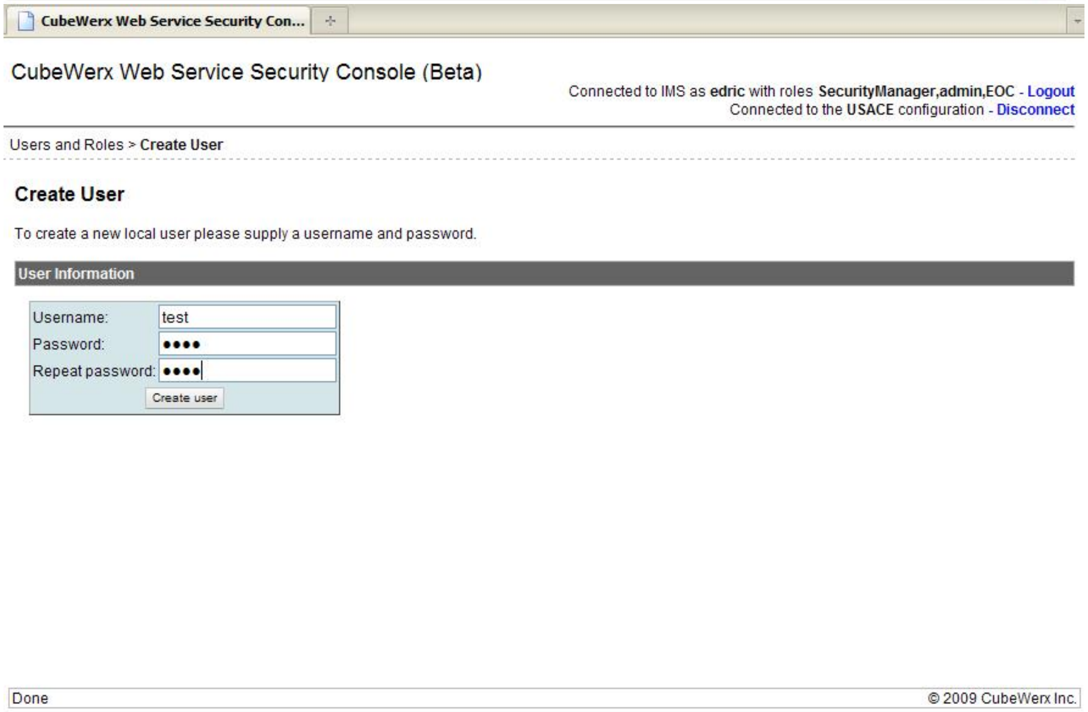
To add a new user or role, click one of the Add links. You can edit or delete existing access rules using the links in the table below.

Existing access control rules + Add User + Add Role

1 - 10 / 27 **Next »** Show 10 Filter Apply Filter

User or role name	Type	Access Rights	Web Services	Delete User/Role
everybody	Special	View XML	Edit Access	
unauth	Special	View XML	Edit Access	
auth	Special	View XML	Edit Access	
edric	User	View XML	Edit Access	Delete
gaetan	User	View XML	Edit Access	Delete
geosync	User	View XML	Edit Access	Delete
glenn	User	View XML	Edit Access	Delete
marc	User	View XML	Edit Access	Delete
mike	User	View XML	Edit Access	Delete
romain	User	View XML	Edit Access	Delete

Done © 2009 CubeWerx Inc.



CubeWerx Web Service Security Console (Beta)

Connected to IMS as **edric** with roles **SecurityManager,admin,EOC** - Logout
Connected to the **USACE** configuration - Disconnect

Users and Roles > **Create User**

Create User

To create a new local user please supply a username and password.

User Information

Username:	test
Password:	••••
Repeat password:	••••

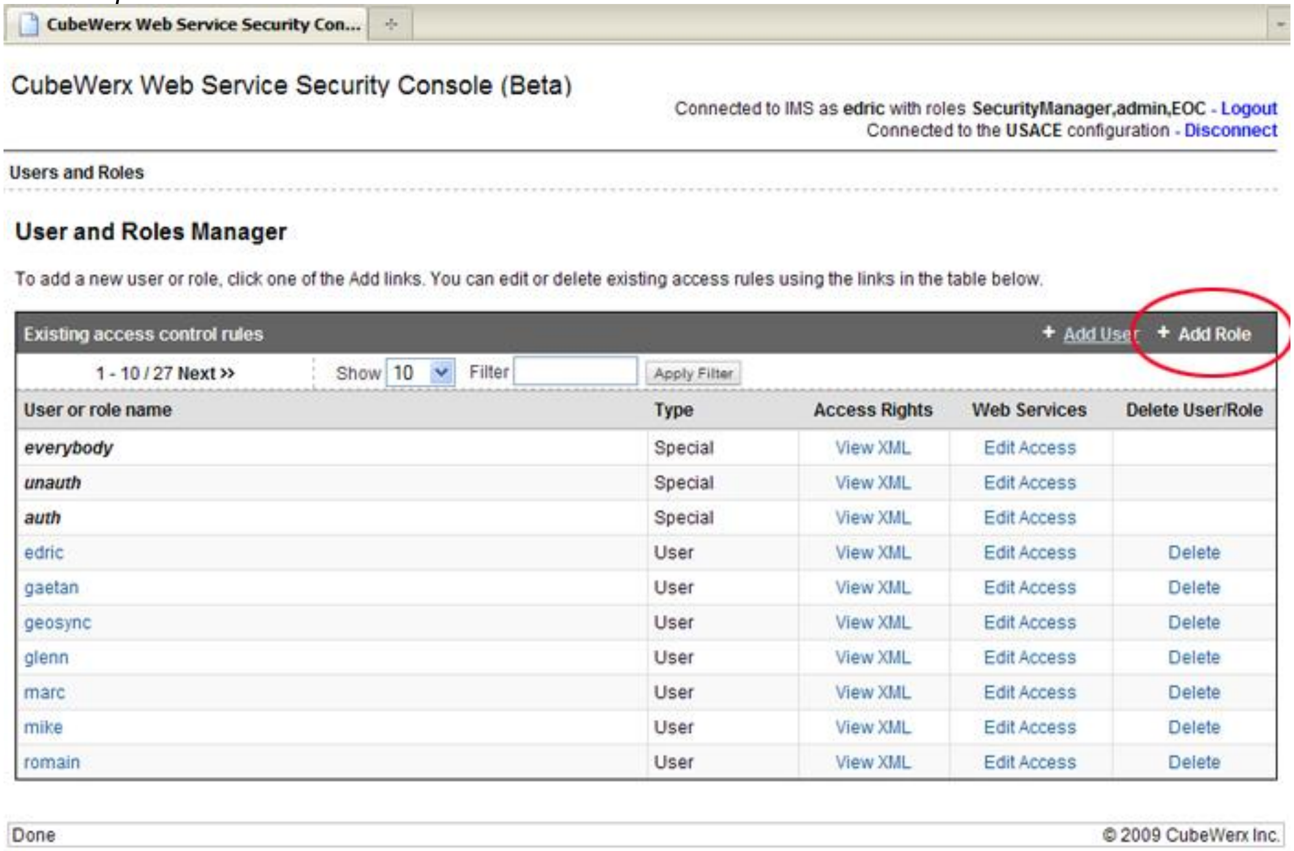
Create user

Done © 2009 CubeWerx Inc.

Use Case 2 - Add Role

Name of use-case	**Add Role**
Actors	Security Manager.
Description	An NSDI Security Manager handles NSDI End Users
Pre-conditions	- A secure NSDI or USACE service exists.
Flow of events	- Security Manager connects to Web Service Security Console (console starts by default in the User and Roles manager) - Manager clicks Add Role, bringing up a dialog where they enter the new role, clicks OK - The new role has been created. The interface automatically moves to the Web Services Access Control screen.
Post-conditions	- A new role has been created

UI Example:



CubeWerx Web Service Security Con...

CubeWerx Web Service Security Console (Beta)

Connected to IMS as **edric** with roles **SecurityManager,admin,EOC** - Logout
Connected to the **USACE** configuration - Disconnect

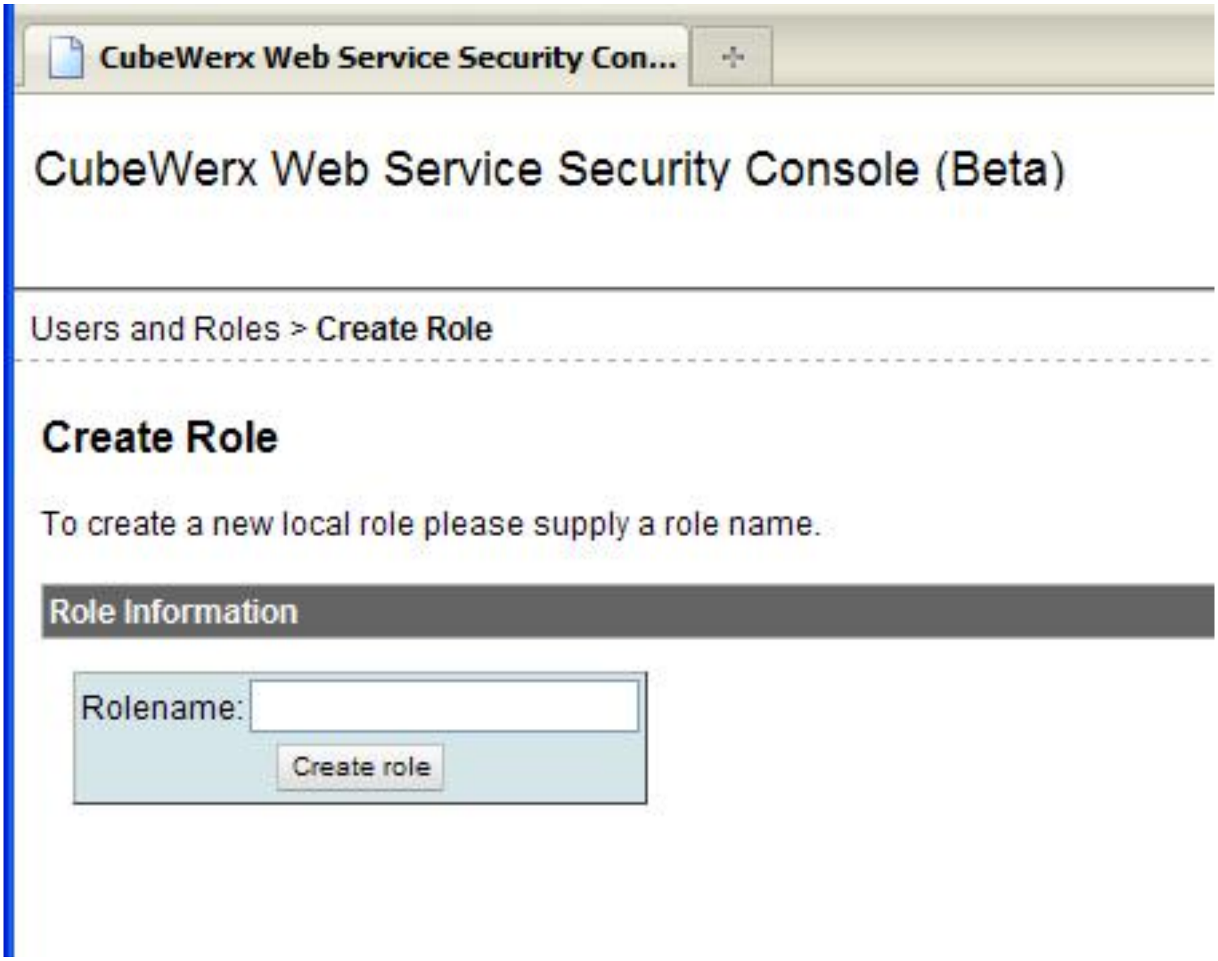
Users and Roles

User and Roles Manager

To add a new user or role, click one of the Add links. You can edit or delete existing access rules using the links in the table below.

Existing access control rules
+ Add User
+ Add Role
1 - 10 / 27 Next >>
Show 10
Filter
Apply Filter

User or role name	Type	Access Rights	Web Services	Delete User/Role
everybody	Special	View XML	Edit Access	
unauth	Special	View XML	Edit Access	
auth	Special	View XML	Edit Access	
edric	User	View XML	Edit Access	Delete
gaetan	User	View XML	Edit Access	Delete
geosync	User	View XML	Edit Access	Delete
glenn	User	View XML	Edit Access	Delete
marc	User	View XML	Edit Access	Delete
mike	User	View XML	Edit Access	Delete
romain	User	View XML	Edit Access	Delete



CubeWerx Web Service Security Console (Beta)

Users and Roles > **Create Role**

Create Role

To create a new local role please supply a role name.

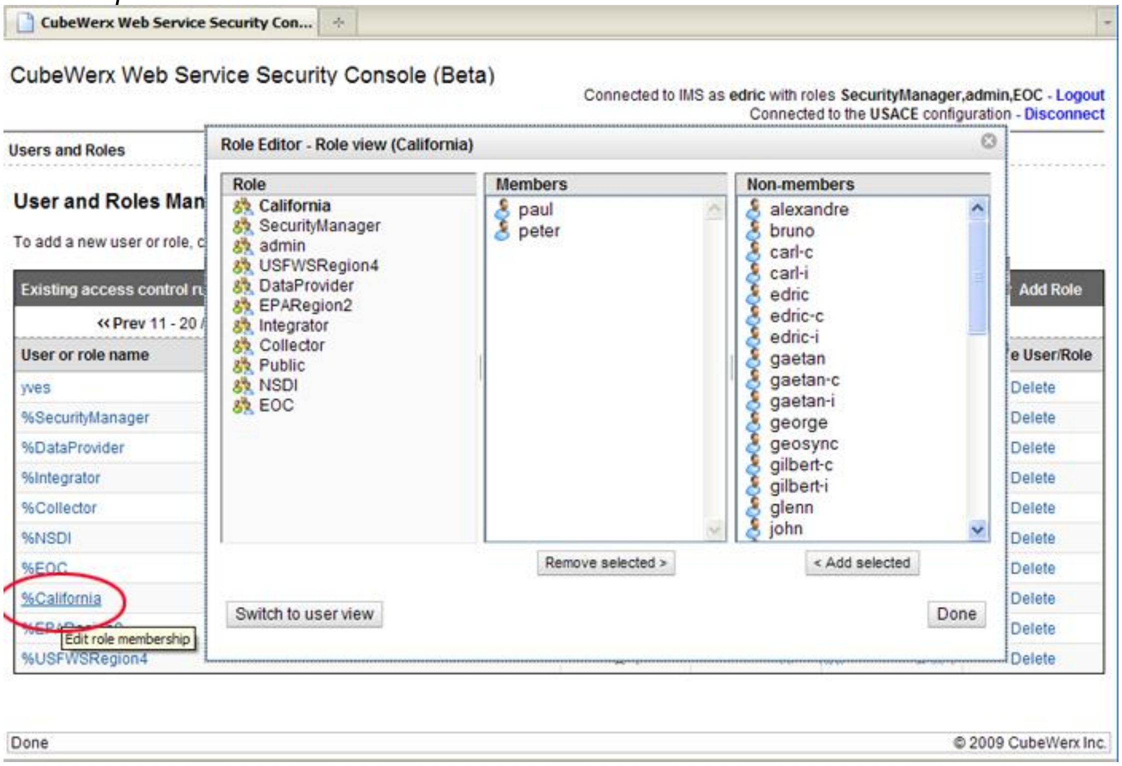
Role Information

Rolename:

Use Case 3 – Add User to Role

Name of use-case	**Add User to Role**
Actors	Security Manager.
Description	An NSDI Security Manager handles NSDI End Users
Pre-conditions	- A secure NSDI or USACE service exists. - At least one NSDI or USACE Role or User exists
Flow of events	- Security Manager connects to Web Service Security Console (console starts by default in the User and Roles manager) - Manager clicks the name of the role they wish to add a user to. - The role manager dialog appears. Manager uses the add/remove buttons to control the membership of the selected Role. - Manager clicks Done to save changes. Dialog disappears and returns to the user manager,
Post-conditions	- The Role membership has been updated

UI Example:



CubeWerx Web Service Security Console (Beta)

Connected to IMS as **edric** with roles **SecurityManager,admin,EOC** - Logout

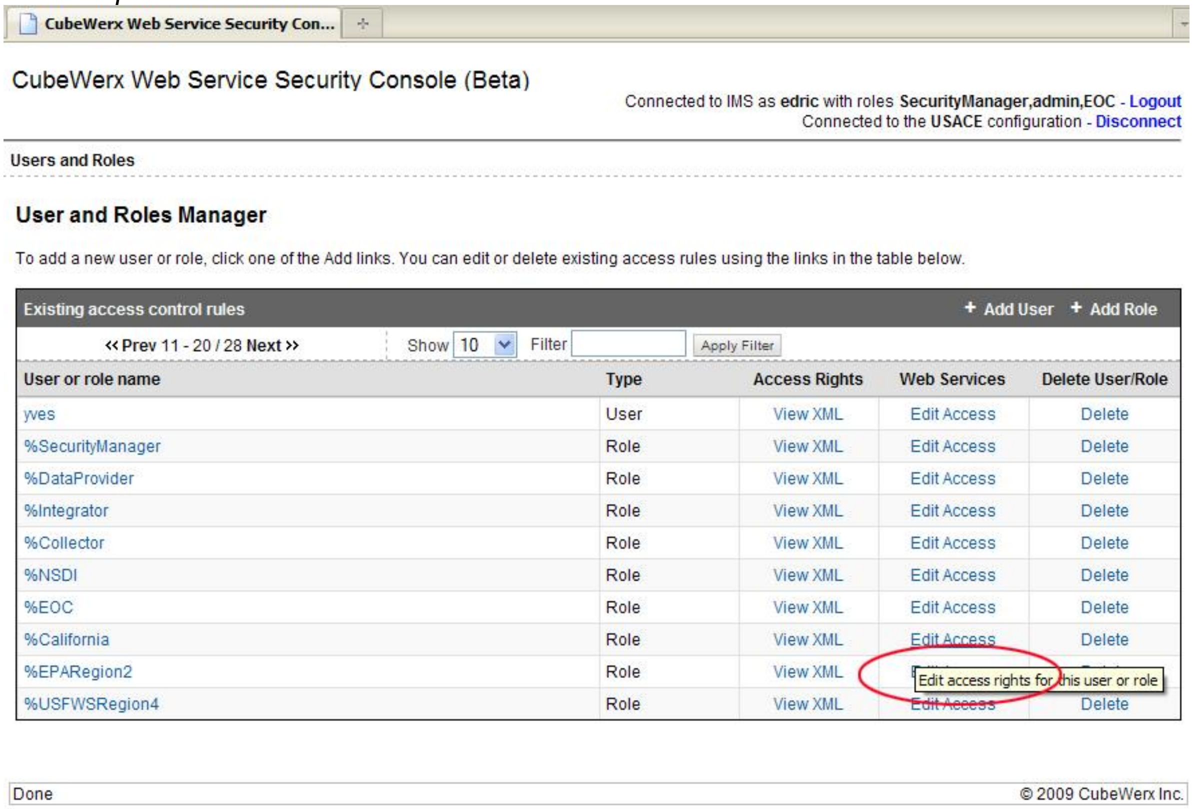
Connected to the **USACE** configuration - Disconnect

Role Editor - Role view (California)

Use Case 4 – Edit Services Access

Name of use-case	**Edit Services Access**
Actors	Security Manager.
Description	An NSDI Security Manager handles NSDI End Users
Pre-conditions	- A secure NSDI or USACE service exists Precondition - At least one NSDI or USACE Role or User exists - Role to be managed has at least one user
Flow of events	- Security Manager connects to Web Service Security Console (console starts by default in the User and Roles manager) - Manager Selects the ‘Edit Access’ Button for the Role they wish to manage. The Web Services Access screen appears. - Manager selects the OGC Services and Service Requests they wish to grant the Role access to. - Manager selects the Save button to confirm actions.
Post-conditions	- The Role now has access to the specified Services and Requests

UI Example:



CubeWerx Web Service Security Console (Beta)

Connected to IMS as **edric** with roles **SecurityManager,admin,EOC** - Logout
Connected to the **USACE** configuration - Disconnect

Users and Roles

User and Roles Manager

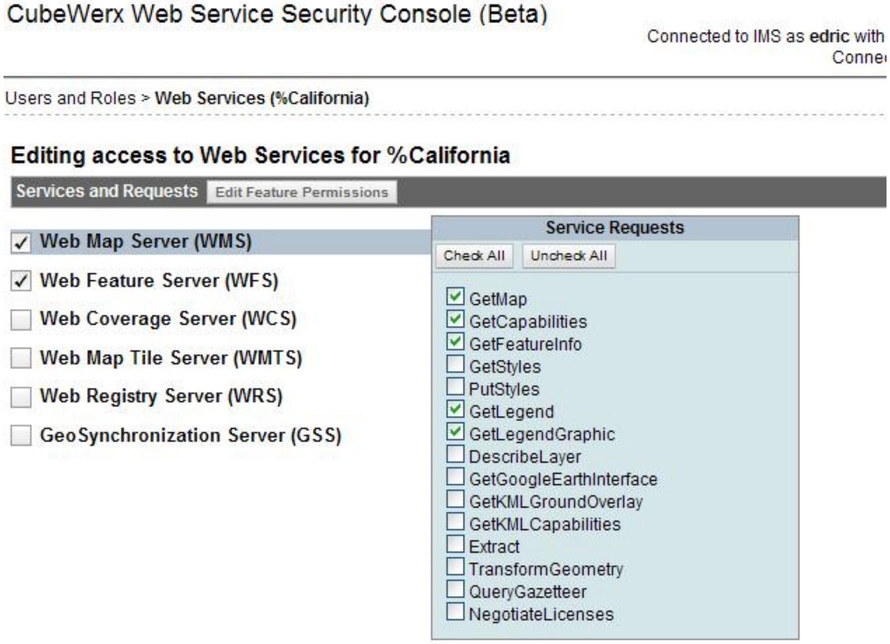
To add a new user or role, click one of the Add links. You can edit or delete existing access rules using the links in the table below.

Existing access control rules + Add User + Add Role

« Prev 11 - 20 / 28 Next » Show 10 Filter Apply Filter

User or role name	Type	Access Rights	Web Services	Delete User/Role
yves	User	View XML	Edit Access	Delete
%SecurityManager	Role	View XML	Edit Access	Delete
%DataProvider	Role	View XML	Edit Access	Delete
%Integrator	Role	View XML	Edit Access	Delete
%Collector	Role	View XML	Edit Access	Delete
%NSDI	Role	View XML	Edit Access	Delete
%EOC	Role	View XML	Edit Access	Delete
%California	Role	View XML	Edit Access	Delete
%EPARegion2	Role	View XML	Edit access rights for this user or role	
%USFWSRegion4	Role	View XML	Edit Access	Delete

Done © 2009 CubeWerx Inc.



CubeWerx Web Service Security Console (Beta)

Connected to IMS as **edric** with
Conne

Users and Roles > **Web Services (%California)**

Editing access to Web Services for %California

Services and Requests | Edit Feature Permissions

- ☑ Web Map Server (WMS)
- ☑ Web Feature Server (WFS)
- □ Web Coverage Server (WCS)
- □ Web Map Tile Server (WMTS)
- □ Web Registry Server (WRS)
- □ GeoSynchronization Server (GSS)

Service Requests

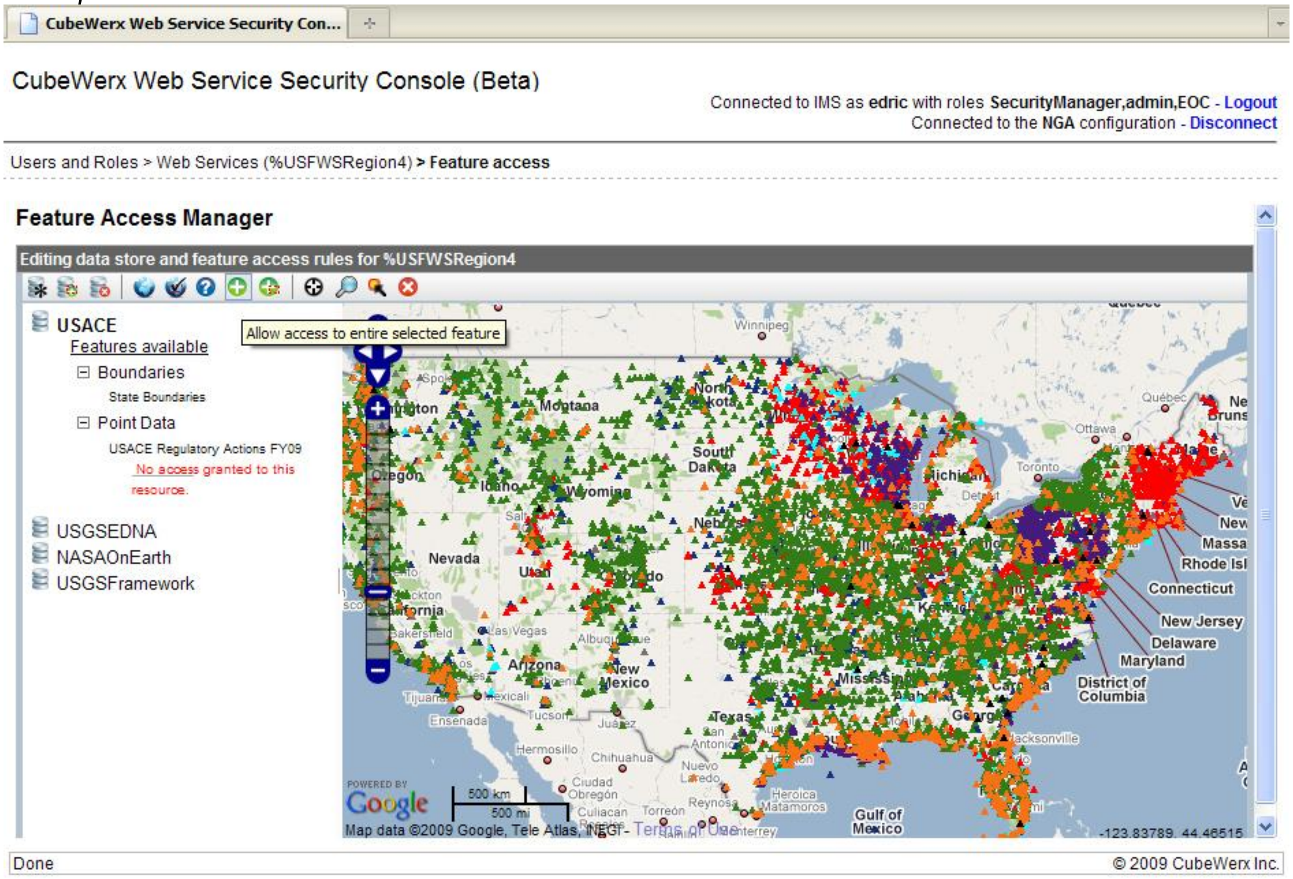
Check All | Uncheck All

- ☑ GetMap
- ☑ GetCapabilities
- ☑ GetFeatureInfo
- □ GetStyles
- □ PutStyles
- ☑ GetLegend
- ☑ GetLegendGraphic
- □ DescribeLayer
- □ GetGoogleEarthInterface
- □ GetKMLGroundOverlay
- □ GetKMLCapabilities
- □ Extract
- □ TransformGeometry
- □ QueryGazetteer
- □ NegotiateLicenses

Use Case 5 - Manage Feature Permissions

Name of use-case	**Manage Feature Permissions**
Actors	Security Manager.
Description	An NSDI Security Manager handles NSDI End Users
Pre-conditions	- A secure NSDI or USACE service - At least one NSDI or USACE Role or User exists - Role to be managed has at least one user - Role has been granted access to the requires OGC Services and Requests for the data they wish to access
Flow of events	- Security Manager connects to Web Service Security Console (console starts by default in the User and Roles manager) - Manager Selects the ‘Edit Access’ Button for the Role they wish to manage. The Web Services Access screen appears. - Manager selects the Edit Feature Permissions button on the Web Services screen. The Feature Access Manager Appears. - Manager Navigates the data store and feature trees on the left of the screen to find the feature they wish to grant access to. - Selects the Green Plus button in the toolbar to grant access to the entire layer. - OR Selects the Green Plus with region button to draw a region on the map interface in which to grant access to the layer - Selects the Save Changes button to confirm.
Post-conditions	- The Role now has access to the specified Feature (within the specified region).

UI Example:



CubeWerx Web Service Security Con...

CubeWerx Web Service Security Console (Beta)

Connected to IMS as **edric** with roles **SecurityManager,admin,EOC** - Logout
Connected to the **NGA** configuration - Disconnect

Users and Roles > Web Services (%USFWSRegion4) > **Feature access**

Feature Access Manager

Editing data store and feature access rules for %USFWSRegion4

Allow access to entire selected feature

- USACE
  - Features available
    - ⊟ Boundaries
      - State Boundaries
    - ⊟ Point Data
      - USACE Regulatory Actions FY09
        - No access granted to this resource.
- USGSEDNA
- NASAOnEarth
- USGSFramework

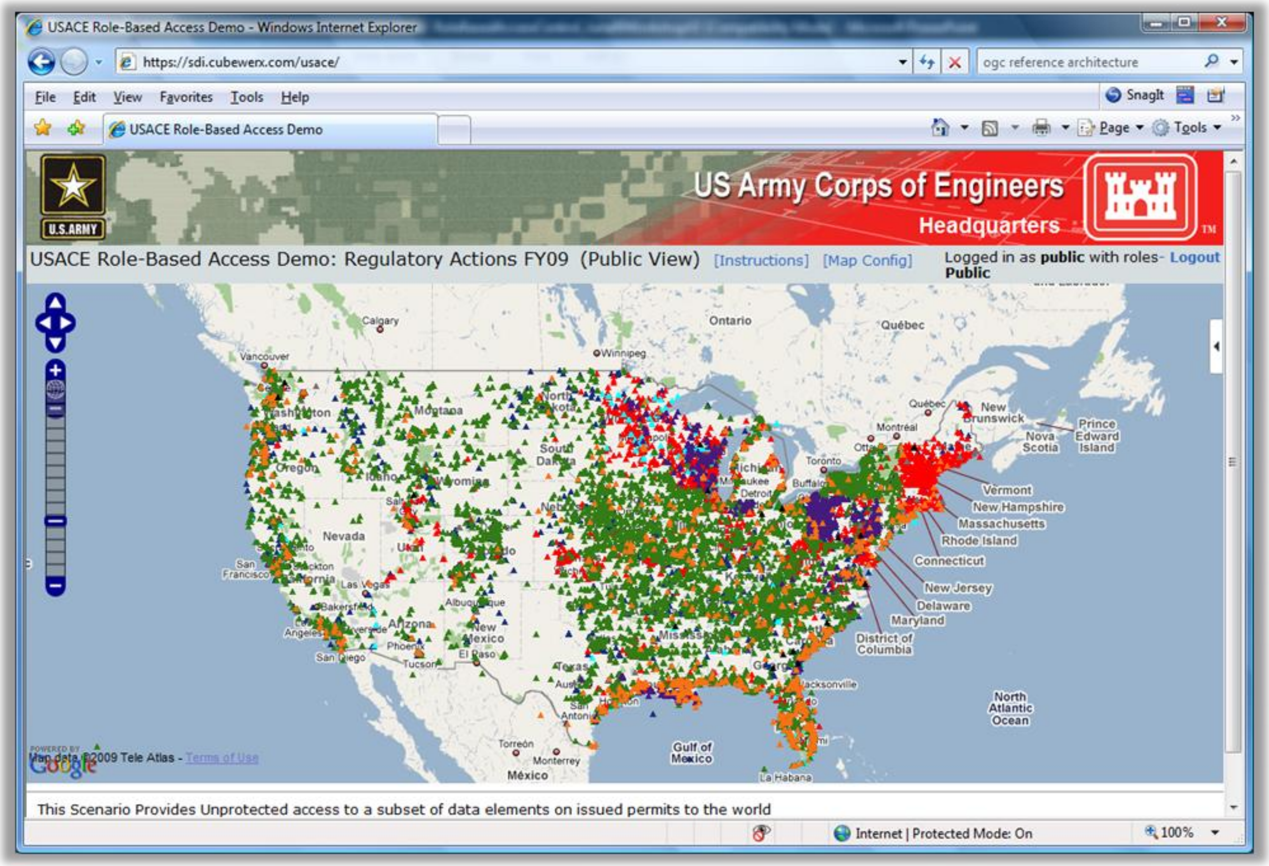
Done

© 2009 CubeWerx Inc.

Use Case 6 – Deploy Data

Name of use-case	**Deploy Data**
Actors	NSDI or USACE Data Provider
Description	An NSDI or USACE Data Provider deploys geospatial data.
Pre-conditions	- Geospatial data exists - At least one NSDI or USACE Role or User exists
Flow of events	- User selects geospatial data - Establishes WMS, WFS, or WCS connected to Internet
Post-conditions	- Geospatial data service and data elements exists for NSDI or USACE access.

UI Example:



USACE Role-Based Access Demo: Regulatory Actions FY09 (Public View) [Instructions] [Map Config]

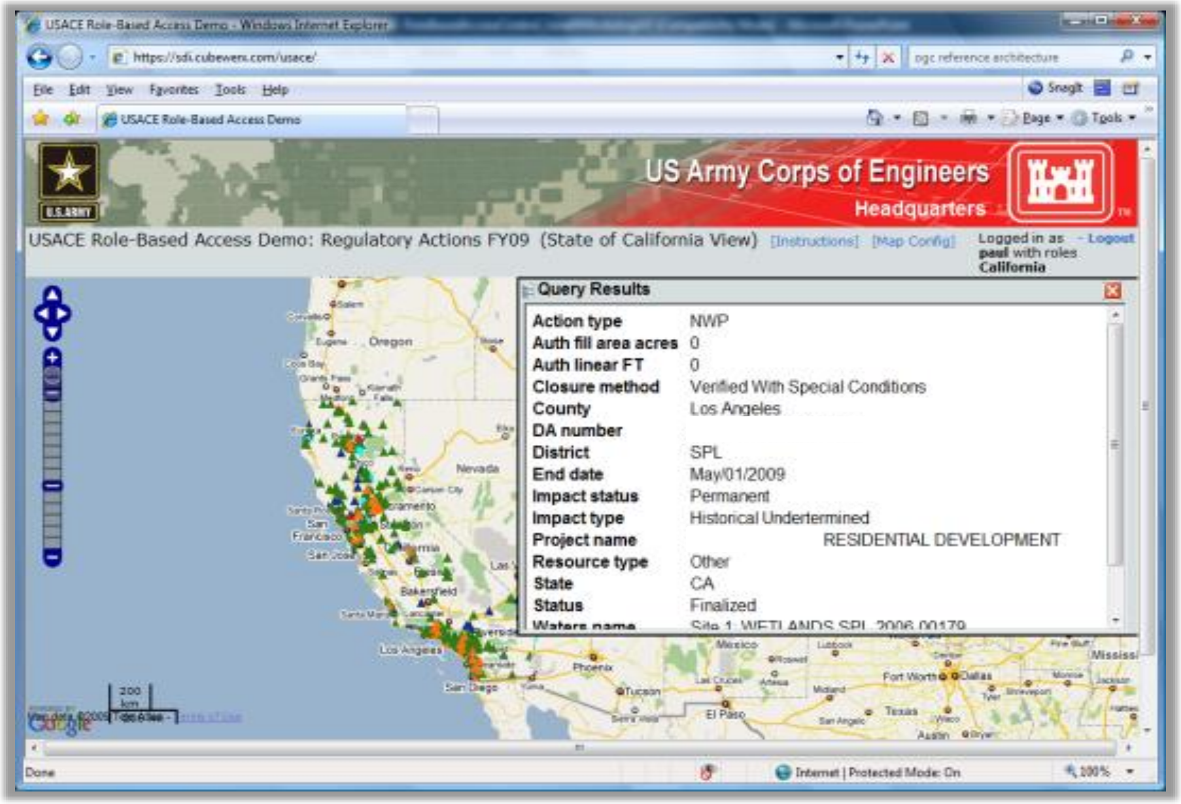
Logged in as **public** with roles- **Logout** **Public**

This Scenario Provides Unprotected access to a subset of data elements on issued permits to the world

Use Case 7 – Access by Geography

Name of use-case	**Access by Geography**
Actors	NSDI End User (Public), NSDI End User (Govt), USACE End User
Description	An End User is granted authenticated access to a consistent view of USACE data over the State of California.
Pre-conditions	- A secure NSDI or USACE service - At least one NSDI or USACE Role or User exists
Flow of events	- User connects to or launches application - User submits username and password. - Appropriate service “requests” and “layers” are presented over constrained geography and Google Maps - User selects data for more info. - User repeats logs out of the application.
Post-conditions	- None

UI Example:


USACE Role-Based Access Demo - Windows Internet Explorer
https://sdi.cubewerx.com/usace/
ogc reference architecture
File
Edit
View
Favorites
Tools
Help
Snagit
USACE Role-Based Access Demo
Page
Tools
U.S. ARMY
US Army Corps of Engineers
Headquarters
Oregon
Nevada
San Francisco
San Jose
Bakersfield
Los Angeles
San Diego
Phoenix
Tucson
El Paso
Fort Worth
Dallas
Texas
Austin
200 km
Done
Internet | Protected Mode: On
100%

USACE Role-Based Access Demo: Regulatory Actions FY09 (State of California View) [Instructions] [Map Config] Logged in as paul with roles California - Logout

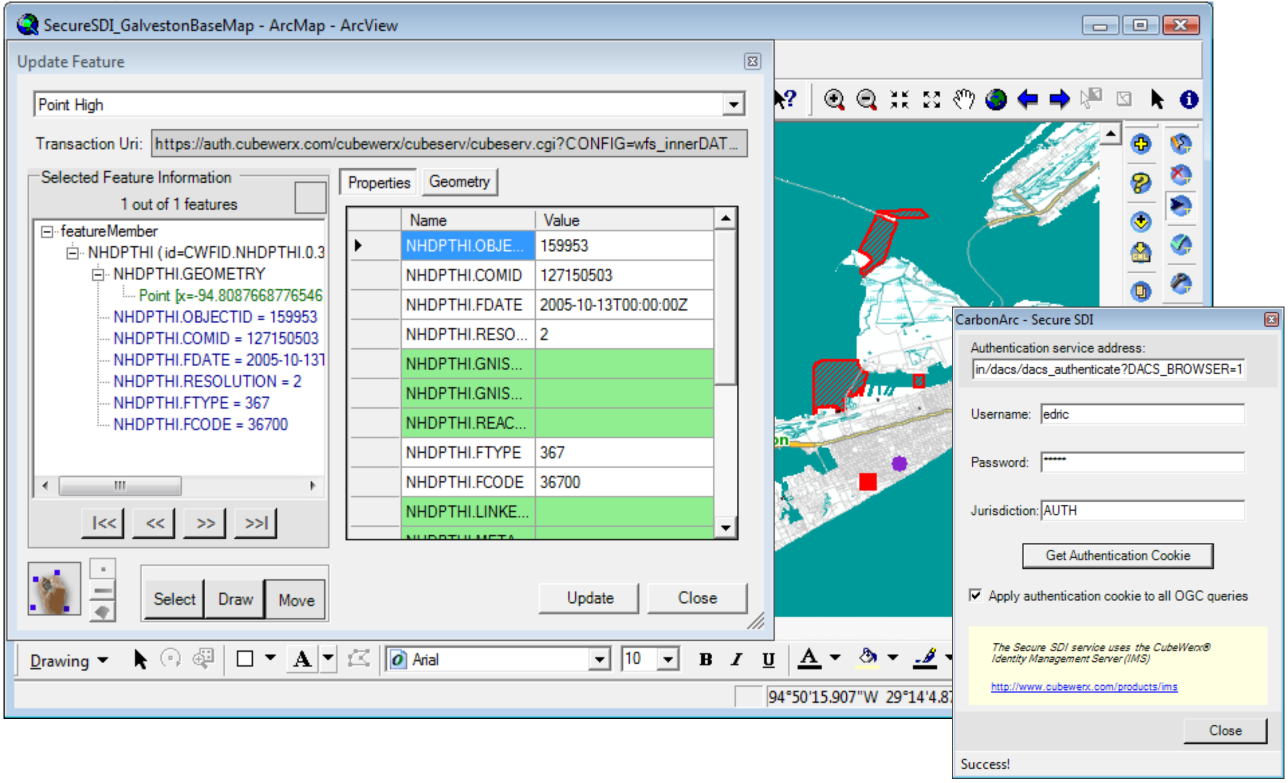
Query Results

Action type	NWP
Auth fill area acres	0
Auth linear FT	0
Closure method	Verified With Special Conditions
County	Los Angeles
DA number	
District	SPL
End date	May/01/2009
Impact status	Permanent
Impact type	Historical Undertermined
Project name	RESIDENTIAL DEVELOPMENT
Resource type	Other
State	CA
Status	Finalized
Waters name	Site 1 WETLANDS SPL 2006 00179

Use Case 8 – Access by Request

Name of use-case	**Access by Request**
Actors	NSDI End User (Govt EOC), USACE End User in EOC
Description	An End User is granted authenticated access to a WFS Transactions requests on USGS data in support of Hurricane response.
Pre-conditions	- A secure NSDI or USACE service - At least one NSDI or USACE Role or User exists
Flow of events	- User connects to USGS Framework WMS and WFS-T with ArcGIS and CarbonArc PRO Extension - User logs in to SDI Access Control Service - User access features to be updated using Manage Transaction Sources dialog - User selects Updates Features - User Commits Transactions to WFS-T
Post-conditions	- NSDI feature data is Updated on Service.

UI Example:



SecureSDI_GalvestonBaseMap - ArcMap - ArcView

Update Feature

Point High

Transaction Uri: https://auth.cubewerx.com/cubewerx/cubeserv/cubeserv.cgi?CONFIG=wfs_innerDAT...

Selected Feature Information

1 out of 1 features

```
⊟ featureMember
   ⊟ NHDPTHI (id=CWFID.NHDPTHI.0.3
      ⊟ NHDPTHI.GEOMETRY
           Point [x=-94.8087668776546
        NHDPTHI.OBJECTID = 159953
        NHDPTHI.COMID = 127150503
        NHDPTHI.FDATE = 2005-10-131
        NHDPTHI.RESOLUTION = 2
        NHDPTHI.FTYPE = 367
        NHDPTHI.FCODE = 36700
```

Name	Value
NHDPTHI.OBJE...	159953
NHDPTHI.COMID	127150503
NHDPTHI.FDATE	2005-10-13T00:00:00Z
NHDPTHI.RESO...	2
NHDPTHI.GNIS...	
NHDPTHI.GNIS...	
NHDPTHI.REAC...	
NHDPTHI.FTYPE	367
NHDPTHI.FCODE	36700
NHDPTHI.LINKE...	

CarbonArc - Secure SDI

Authentication service address: in/dacs/dacs_authenticate?DACS_BROWSER=1

Username: edric

Password: ******

Jurisdiction: AUTH

☑ Apply authentication cookie to all OGC queries

The Secure SDI service uses the CubeWerx® Identity Management Server (IMS)

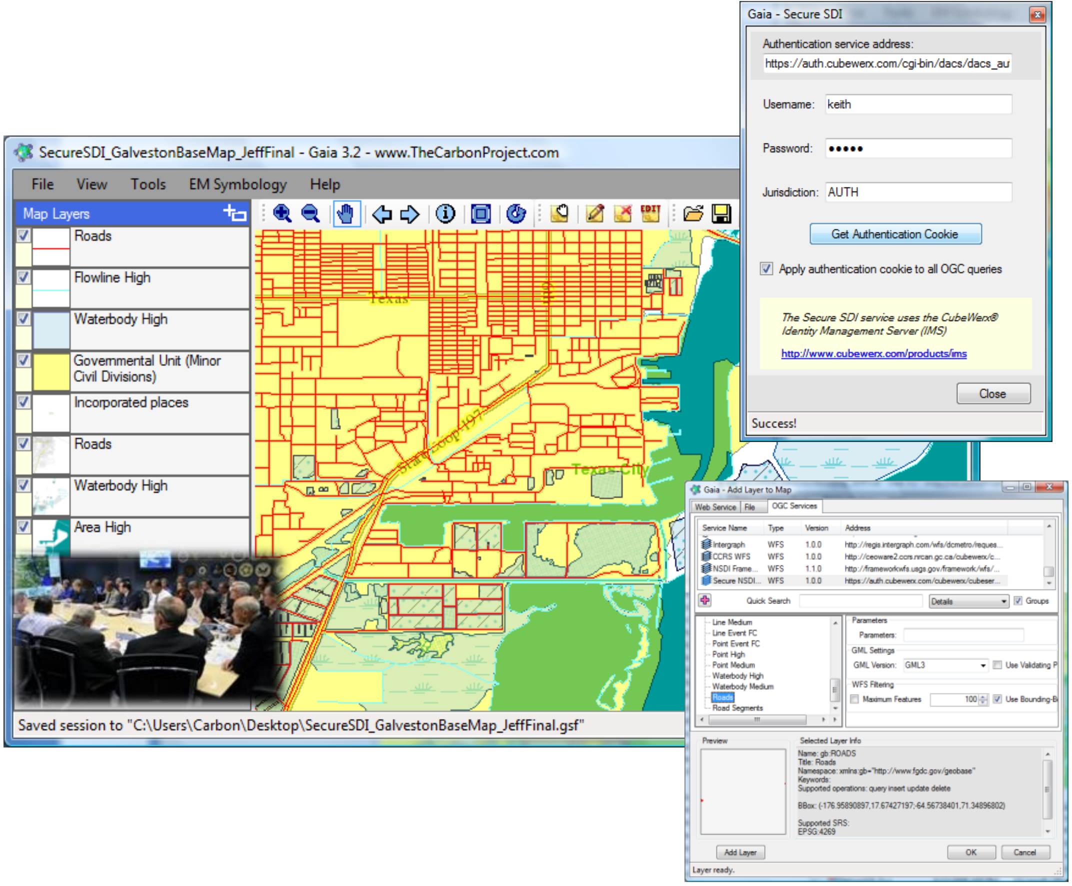
http://www.cubewerx.com/products/ims

Success!

Use Case 9 – Access by Layer

Name of use-case	**Access by Layer**
Actors	NSDI End User (Govt EOC), NSDI End User (Public)
Description	An End User is granted authenticated access to Features via USGS WFS data in support of Hurricane response.
Pre-conditions	- A secure NSDI or USACE service supporting WMS and WFS - At least one NSDI or USACE Role or User exists.
Flow of events	- User connects to NSDI WMS using Gaia SDI Platform - User logs in to SDI Access Control Service - User selects NSDI WFS to be displayed over Galveston Island. - User accesses features to be displayed over Galveston Island. - User saves features
Post-conditions	- Features are available for use on desktop application.

UI Example:



SecureSDI_GalvestonBaseMap_JeffFinal - Gaia 3.2 - www.TheCarbonProject.com

Saved session to "C:\Users\Carbon\Desktop\SecureSDI_GalvestonBaseMap_JeffFinal.gsf"

Gaia - Secure SDI

Authentication service address: https://auth.cubewerx.com/cgi-bin/dacs/dacs_au

Username: keith

Password: •••••

Jurisdiction: AUTH

☑ Apply authentication cookie to all OGC queries

The Secure SDI service uses the CubeWerx® Identity Management Server (IMS)

http://www.cubewerx.com/products/ims

Success!

Gaia - Add Layer to Map

Service Name	Type	Version	Address
Intergraph	WFS	1.0.0	http://regis.intergraph.com/wfs/dcmetro/reques...
CCRS WFS	WFS	1.0.0	http://ceoware2.ccrs.nrcan.gc.ca/cubewerx/c...
NSDI Frame...	WFS	1.1.0	http://frameworkwfs.usgs.gov/framework/wfs/...
Secure NSDI...	WFS	1.0.0	https://auth.cubewerx.com/cubewerx/cubeser...

Quick Search: Details ☑ Groups

Parameters

Parameters:

GML Settings

GML Version: GML3 □ Use Validating P

WFS Filtering

□ Maximum Features 100 ☑ Use Bounding-B

Selected Layer Info

Name: gb:ROADS
Title: Roads
Namespace: xmlns:gb="http://www.fgdc.gov/geobase"
Keywords:
Supported operations: query insert update delete

BBox: (-176.95890897,17.67427197;-64.56738401,71.34896802)

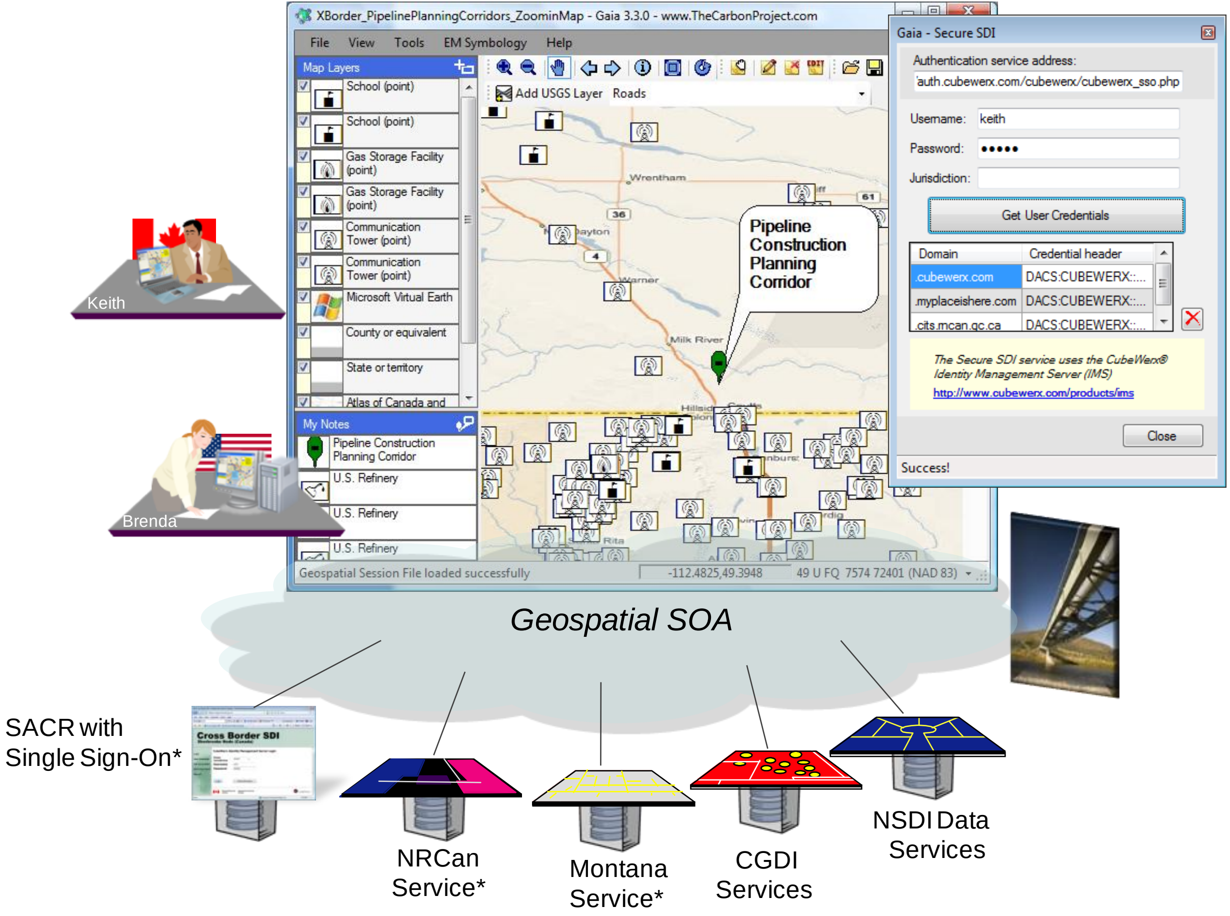
Supported SRS:
EPSG:4269

Layer ready.

Use Case 10 – Single Sign-On

Name of use-case	**Single Sign-On**
Actors	NSDI End User
Description	An End User is granted authenticated access to Features via WFS in the United States and Canada in support of Project Planning.
Pre-conditions	- Secure NSDI or Canadian services supporting WFS - At least one NSDI Role or User exists .
Flow of events	- User logs in to SDI Access Control Service - User selects NSDI WFS to be displayed over Montana. - User selects CGDI WFS to be displayed over Canada. - User styles and saves features for project planning.
Post-conditions	- User is logged into multiple security jurisdictions.

UI Example:



XBorder_PipelinePlanningCorridors_ZoominMap - Gaia 3.3.0 - www.TheCarbonProject.com

Geospatial Session File loaded successfully   -112.4825,49.3948   49 U FQ 7574 72401 (NAD 83)

Gaia - Secure SDI

Authentication service address: 'auth.cubewerx.com/cubewerx/cubewerx_sso.php

Username: keith

Password: •••••

Jurisdiction:

Domain	Credential header
.cubewerx.com	DACS:CUBEWERX::...
.myplaceishere.com	DACS:CUBEWERX::...
.cits.mcan.gc.ca	DACS:CUBEWERX::...

The Secure SDI service uses the CubeWerx® Identity Management Server (IMS)
http://www.cubewerx.com/products/ims

Success!

Appendix B - OGC GeoDRM/Access Control Framework CrossWalk

This document provides a brief review and comparison of the Geospatial Digital Rights Management Reference Model (GeoDRM RM), an abstract specification for the management of digital rights in the area of geospatial data and services and the CubeWerx Identity Management Service, a distributed *access control framework* to facilitate secure sharing of web resources. The GeoDRM RM is Topic 18 of the OpenGIS® Abstract Specification.

It should be noted that the OGC GeoDRM document is not an implementation specification, therefore direct comparisons of Access Control Framework architecture with elements of the design document are not always possible, although after careful review we believe that the implementation of Access Control Framework does fit the model described in the OGC document quite well. The OGC document defines a "roadmap" of GeoDRM design principles. The elements of the road map are described below (direct from the document), along with a response from CubeWerx indicating how we do (or do not fit) into this model.

Rights Model

The definition of an abstract Rights Model is the topic of the GeoDRM RM. It defines the basis for developing a geo-specific Rights Expression Language as well as other specifications necessary to establish a GeoDRM-enabled SDI. The document goes on to describe a very high level view of an abstract rights model.

Although no direct comparison can be drawn between elements of this model and implemented features of The Access Control Framework, IMS does fit into the general architecture suggested by the model.

Rights Expression Language

The GeoDRM RM provides the capabilities to express usage rights in the form of a machine-readable and machine-processible representation. The definition of a geo-specific Rights Expression Language is not part of the document, but is to be defined upon the Rights Model declared in this specification.

The Access Control Framework uses an XML based ACL (Access control list) language, which supports the model described in the GeoDRM document.

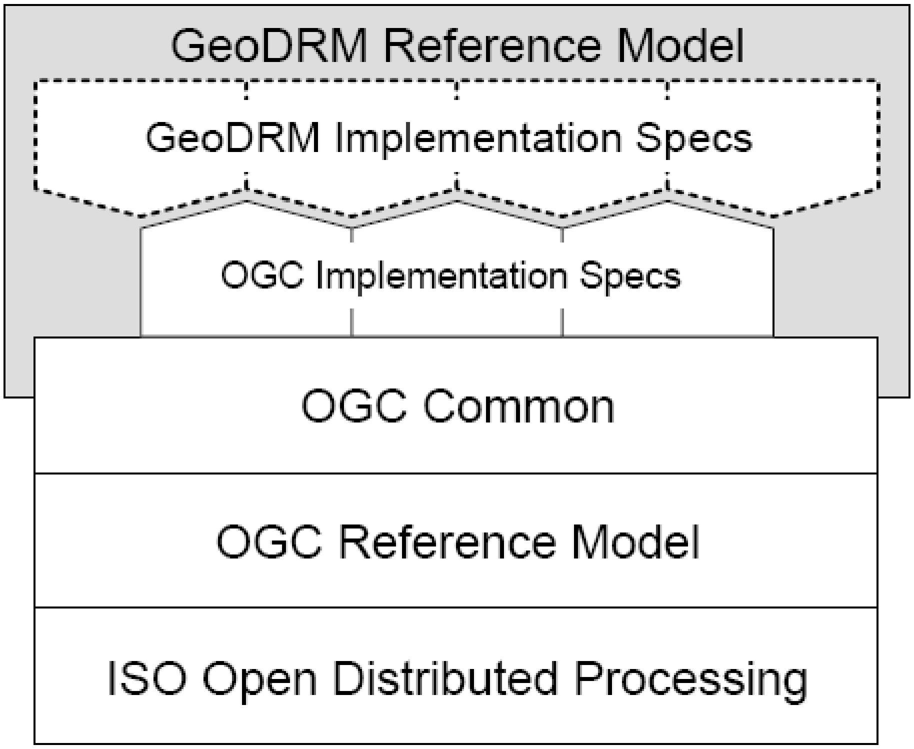


Figure 1: GeoDRM Reference Model Context

Encryption

The GeoDRM RM includes required functionality to protect a GeoDRM-enabled SDI against fraud. First, encryption enables the protection of a license so that it cannot be modified by an adversary in order to obtain additional rights. Second, encryption is also useful to protect the digital geographic content against unlicensed use. An example from the music industry exists, where the encrypted music file can only be decrypted (and played) by a certified software or hardware device. Because security and trust are not geo-specific, no standardization is planned from this WG.

The Access Control Framework requires the use of SSL (Secure Socket Layer) for all client-server communication. Credentials are encrypted with a highly secure algorithm.

Enforcement and Authorization

The rights expressed in a GeoLicence need to be enforced. In this specification, this package functionality is represented by the "Gate Keeper" metaphor. The acceptance or denial decision for a particular request (with its associated licenses) is based on the authorization decision, as it is derived by the authorization engine. Because enforcement and authorization is geo-specific, the appropriate standardization is upcoming work to be based on this specification.

The Access Control Framework implements this model. Every request sent through the web server for a DRM protected resource is routed to the access control module for verification of credentials and rights, i.e., the service first verifies that the user is who he says he is, then validates his right to access the chosen resource against the access control rules. No standardization currently exists for expressing geo-data access rights. The Access Control Framework uses a simple and flexible XML based grammar.

Trust

Every type of business relationship that has been represented in an electronic way needs a mechanism to differentiate between reliable and unreliable partners. In that sense, trust tells a relying partner that the other behaves in a certain predictable (loyal) way. One mechanism to establish trust between entities in an SOA can be done by adding authenticity information on the digital content that is been exchanged between the partners. This mechanism, typically called a Digital Signature, is not geo-specific and therefore is not a relevant topic for standardization by this WG.

The focus on the 2008 CAP Project is Role-based Access Control, and The Access Control Framework does not implement digital signing of content.

License Verification

The GeoDRM RM defines the functionality that is required to validate a license. The license verification has to occur before the rights of the license can be enforced. Because document authentication is not geo-specific, it is not a topic for standardization by this WG.

The Access Control Framework uses an authentication and access control model, as opposed to a traditional license model, therefore access control is enforced at the user level, not the license level.

Authentication

The basic requirement for trust, license verification and enforcement/authorization is proof of identity, as it is provided by the functionality of this package. Different international standards, which define how to enable this functionality, exist. Because authentication is not geo-specific, it is not a topic for standardization by this WG.

The Access Control Framework uses an abstract authentication model that allows it to piggy-back on nearly any existing authentication method LDAP/username, password/Certificates etc). The administrator merely has to create the linkage between their existing authentication framework and IMS.

Additional Analysis – To Be Provided