CubeWerx USA

US Army Corps
of Engineers®

2008 NSDI Cooperative Agreement Program Category 2: Best Practices in Geospatial Service Oriented Architecture (SOA)

Role-based Access Control - Best Practices for Geospatial SOA

Interim Report

Presented To:

NSDI

October 17, 2008

NSDI Cooperative Agreements Program
Category 2: Best Practices in Geospatial Service Oriented Architecture (SOA)
Interim Report

Date: October 17, 2008

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, Managing Director
Phone: 703 491 9543
Email: jharrison@cubewerx.com

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

Edric Keighan, President & CEO
CubeWerx, Inc.
Phone: 819.771.8303
Email: ekeighan@cubewerx.com
Internet Address: http://www.cubewerx.com

Executive Summary

This project is developing Best Practices for one of the most important, but least understood, areas of Geospatial SOA – Role-based Access Control. Development is being coordinated with other 2008 Category 2 recipients and will satisfy multi-agency requirements through the modeling and deployment of business processes and related data and service components. Documentation of 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 is the advancement of technology that can support regulatory data interoperability between organizations like USACE, EPA and USFWS. Basic goals of the CAP Category 2 Best Practices in Geospatial SOA effort are summarized in Figure 1 below.

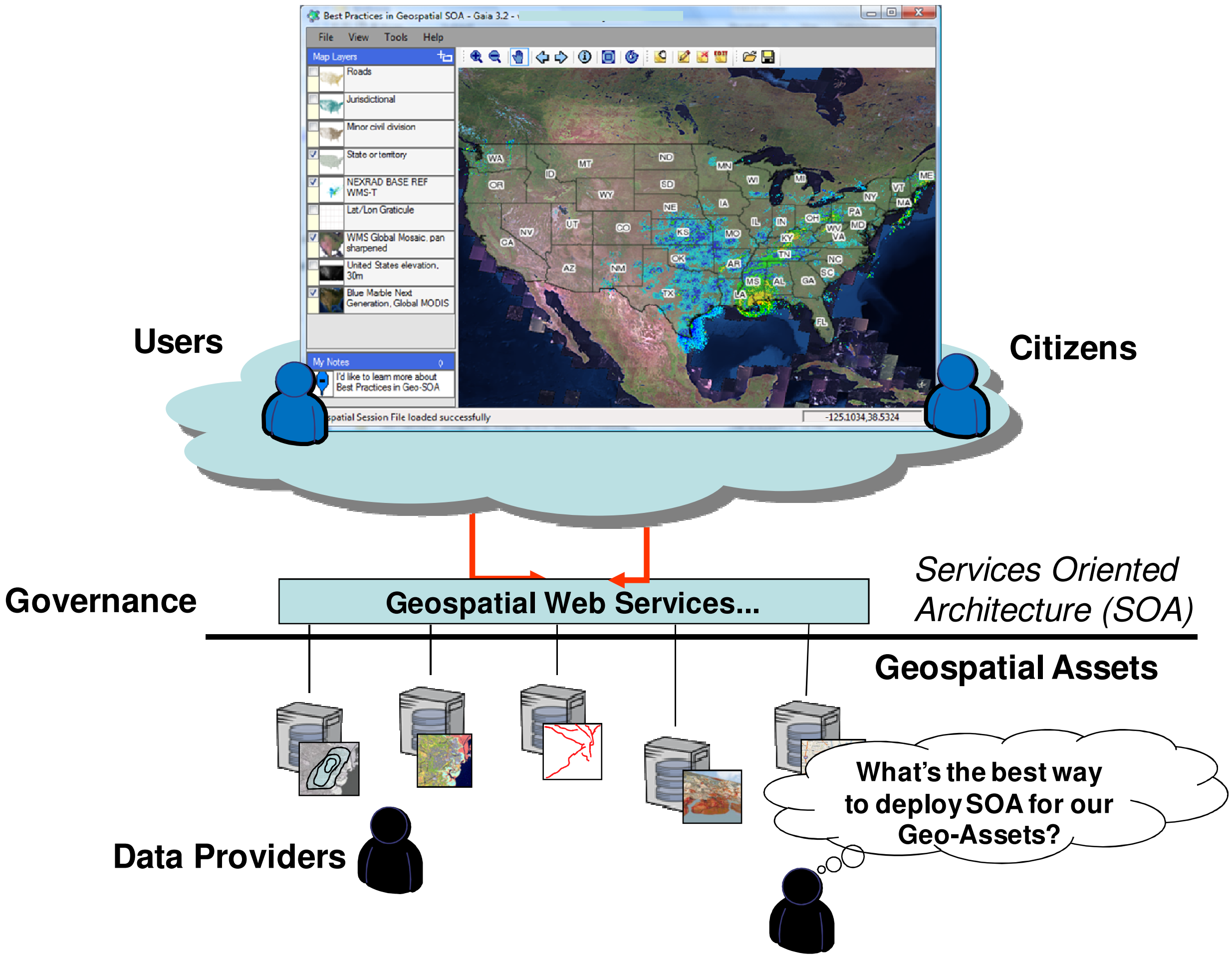

Best Practices in Geospatial SOA - Gaia 3.2 -
File
View
Tools
Help
Map Layers
☐ Roads
☐ Jurisdictional
☐ Minor civil division
☑ State or territory
☑ NEXRAD BASE REF WMS-T
☐ Lat/Lon Graticule
☑ WMS Global Mosaic, pan sharpened
☐ United States elevation, 30m
☑ Blue Marble Next Generation, Global MODIS
My Notes
I'd like to learn more about Best Practices in Geo-SOA
WA
OR
ID
MT
WY
ND
SD
NE
MN
WI
MI
IA
NV
CA
UT
CO
KS
MO
IL
IN
OH
PA
NY
VT
ME
MA
WV
VA
MD
KY
TN
NC
SC
GA
AL
MS
LA
AR
OK
TX
NM
AZ
FL
spatial Session File loaded successfully
-125.1034,38.5324
Users
Citizens
Governance
Geospatial Web Services...
Services Oriented Architecture (SOA)
Geospatial Assets
What's the best way to deploy SOA for our Geo-Assets?
Data Providers

Figure 1 – Best Practices in Geospatial SOA CAP projects for 2008 are designed to help document best practices and educate federal agencies on design, implementation, and application of government-wide services for Geospatial LoB.

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[2] where loosely affiliated parties collaborate on maintenance of shared geospatial data resources.

[1] http://colab.cim3.net/file/work/geocop/ProfileDocument/FEA_Geospatial_Profile_v1_1.pdf
[2] http://www.opengeospatial.org/standards/requests/43

To meet this challenge, this project is defining and documenting Best Practices in Geospatial SOA for Role-based Access to GeoData as a key component of USACE and NSDI Business Process requirements. This project leverages CubeWerx's investment in developing solutions to solve this important security challenge. Specifically, CubeWerx is deploying 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.

The project is leveraging this CubeWerx investment, called the Identity Management Service (IMS), as part of the Operational NSDI. IMS is a framework to manage identities and enforce 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 Access Control Rules (ACL). 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 will build on this capability and design, deploy, and document reusable services and Best Practices for Role-based Access to GeoData within NSDI enterprises. In this project, our team is providing expertise related to current trends and developments in geospatial services oriented architectures, and collaborating 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.

While the project demonstrates functionality specific to USACE's needs, it also demonstrates capabilities 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. It is the goal of the CubeWerx/USACE team to collaboratively document Best Practices and the implemented operating capability to address common requirements of the Geospatial Line of Business across government.

Project Narrative

After the project kickoff, CubeWerx USA established a test Identity Management Service and a secure version of the NSDI WFS located at http://frameworkwfs.usgs.gov/ for 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. 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 CubeWerx CubeSERV product.
7. NSDI WFS returns appropriate Features.

This scenario is depicted in Figures 2 and 3 below.

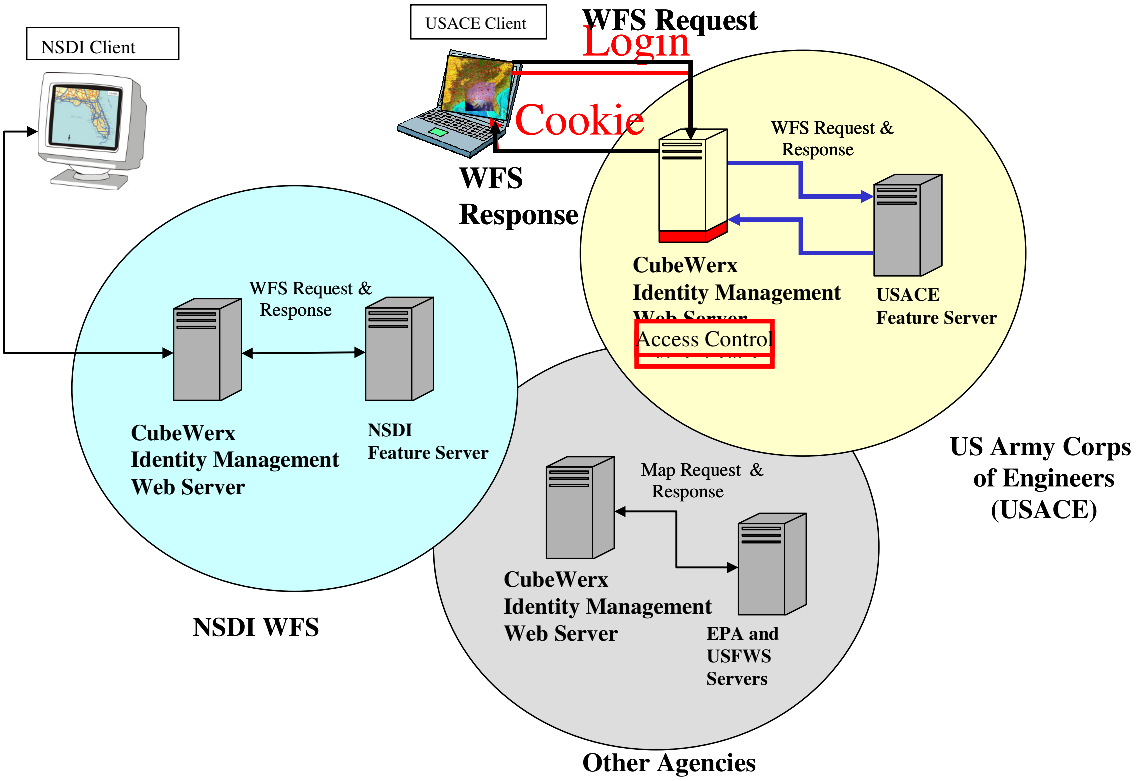


Figure 2 – The basic access control scenario includes a USACE Client accessing resource at USACE

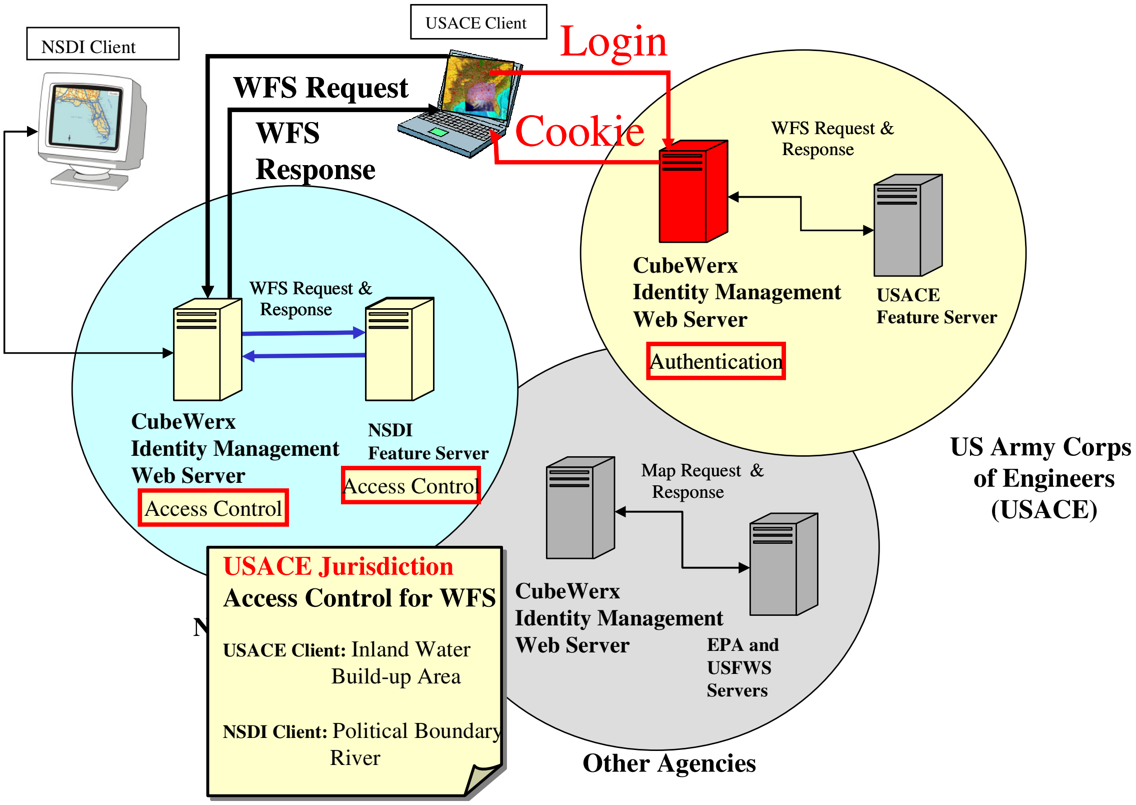


Figure 3 – An alternate scenario includes a USACE Client accessing resource at USACE and NSDI

The project also began developing a set of basic ‘access control rules’ for geospatial web services in order for the IMS to 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 ("*Keith is an EOC User*") or with a **group** whose membership is known throughout the system (e.g., "*Keith is currently working on Project Ike*"). Access control rules at any NSDI organization can refer to these roles (e.g., "*Grant access to any EOC User*") and groups (e.g., "*Grant access to any member of Project Ike*").

Because rules will refer to user roles and names ("*Keith the EOC User*"), IMS provides a way to name users and mechanisms to manage user identities, including the means by which users can be authenticated. In this project 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. To support this process IMS 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 for example.

SOA Definitions and Approach

In this project CubeWerx USA is using 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, Image Matter and Indiana University. The terms and definitions were taken from authoritative sources, and the references to those sources are included in the listings. We will continue to add to the list and refine the individual definitions throughout the duration of the project.

Requirements and Process Definition

CubeWerx USA is following the general development pattern agreed upon by the three 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.

Upon receiving funding, we reviewed the business processes needed by the US Army Corp of Engineers (COE) and began documenting these in a use case format agreed to by the Category 2 project participants. We began reviewing the Use Cases with USACE program managers and data specialists. Information gathered provided us sufficient data to develop detailed use cases for system interactions. Specifically, after reviewing the basic scenario we assessed there are at least six potential system Actors involved in Role-based Access Control Use Cases.

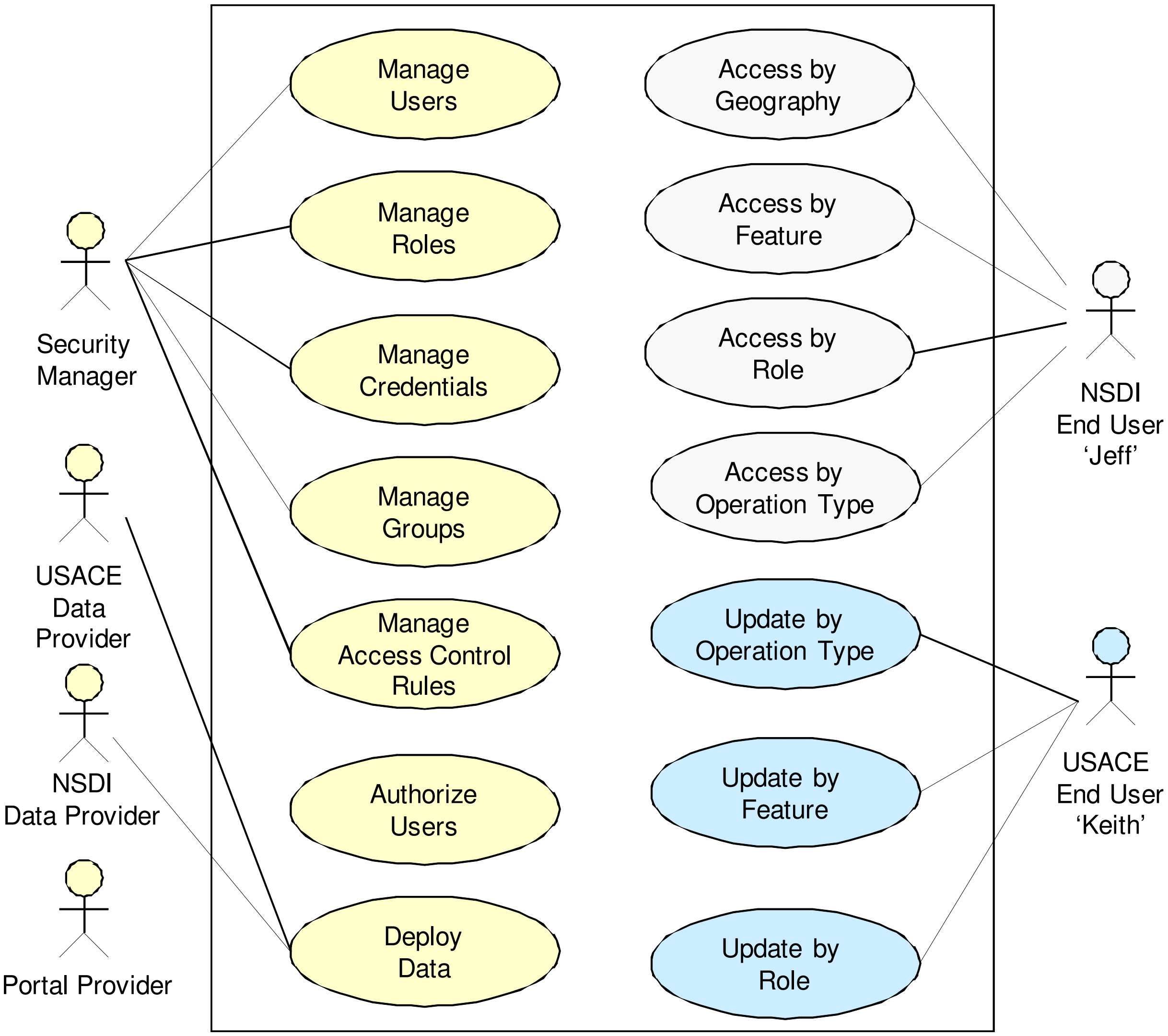


Figure 4 – Initial draft of Role-based Access Control Use Case Diagram. NSDI 'Producer' Actors are depicted on the left of the IMS system and NSDI 'Consumer' Actors on the right.

These Actors include:

<u>USACE Data Provider</u>

A USACE 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.

<u>NSDI Data Provider</u>

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

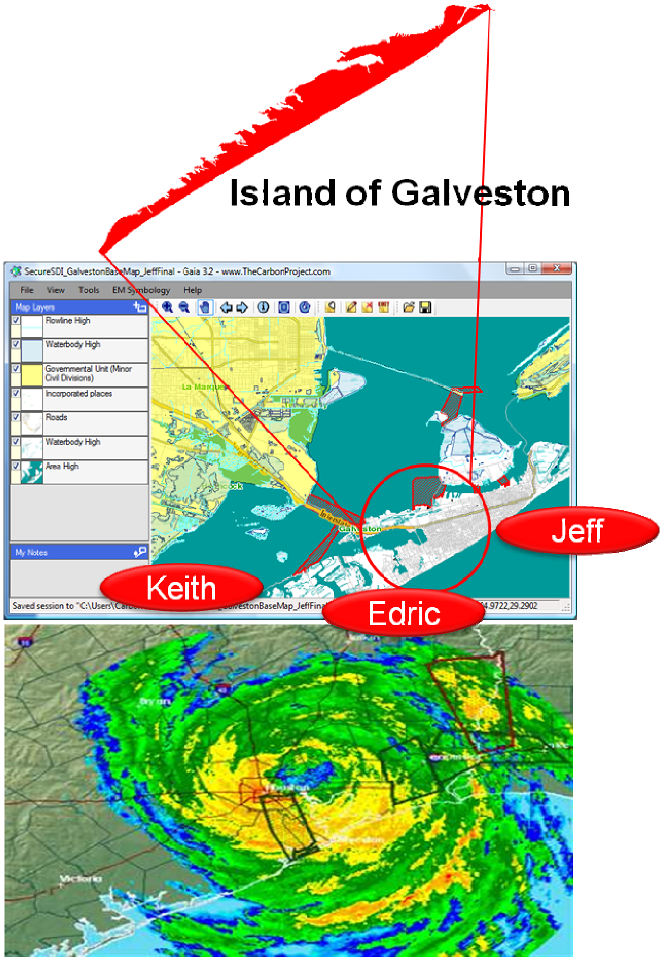
End users not in USACE that wish to discover, view, and obtain current feature datasets which may cover any part of the United States but which are customized to the user’s area of interest.

eGIS Portal Provider

A USACE “eGIS” portal provider who supports user access to local, regional or national feature datasets.

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.



Our effort assessed that these Actors engage in at least 14 Use Cases for Role-based Access Control including those documented in Figure 4. These Uses Cases are being refined in coordination with USACE representatives. To further refine the Use Cases, Best Practices and Access Control Rules we developed a test scenario involving response to a Hurricane event along the Gulf coast of the United States. The scenario included three test Roles –

- NSDI User – ‘Jeff’
- USACE EOC User – ‘Keith’
- NSDI DataProvider – ‘Edric

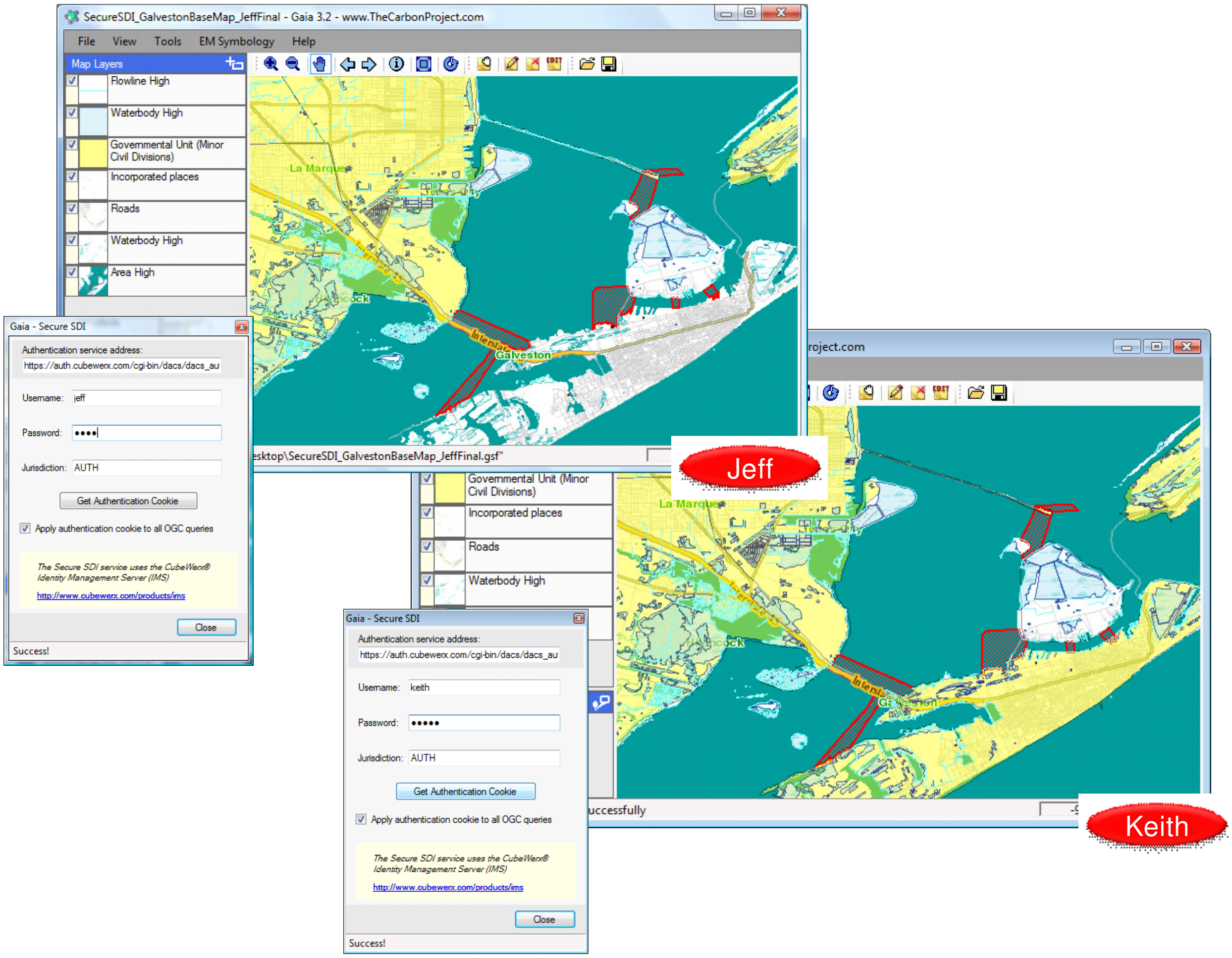
The scenario tested Access Control by *Role, Geography, Feature and OGC Operation*. To support scenario development and system testing we engaged The Carbon Project (www.thecarbonproject.com) to extend its

NSDI viewer, Gaia 3.2[3], 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 5 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 1.6. This tool is available as a free download from –

http://www.thecarbonportal.net/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=4



Gaia - Secure SDI

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

Username: jeff

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!

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!

Figure 5 - To further refine the Use Cases, Best Practices and Access Control Rules we developed a test scenario involving response to a Hurricane event along the Gulf coast of the United States.

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

To support Community Outreach and Collaboration with other Category 2 participants in defining common SOA definitions, modeling approach and deployment strategies CubeWerx USA led the development and delivery of a briefing for GIScience 2008 in Park City Utah on Sept 23, 2008 (http://www.giscience.org/index.php). The briefing, titled “Best Practices in Geospatial SOA” was delivered in support of the “Design of Service-Oriented Architecture (SOA) for Geospatial Science Workshop”.

Figure 6 – The CAP Category 2 team supported the SOA Workshop at GIScience 2008 in Park City Utah on Sept 23, 2008, shown here being led by Workshop organizers Xuan Shi (Georgia Institute of Technology) and Robert Raskin (Jet Propulsion Laboratory)

Our work in the next performance period will focus on collaboratively documenting Best Practices using the test framework developed during the reporting period.