



SECURING GEOSPATIAL INFORMATION

GEOSPATIAL CONTENT AND SERVICE PROVIDERS FREQUENTLY NEED TO CONTROL WHO IS ACCESSING THEIR CONTENT. SUCH CONTROL MAY BE NECESSARY TO ENSURE PROFITS, OR TO RESPECT AGREEMENTS WITH OTHER PROVIDERS IN THE VALUE CHAIN, OR TO RESPECT PRIVACY RIGHTS, OR TO REDUCE RISKS TO INFORMATION, LIVES, REAL PROPERTY OR NATIONAL SECURITY, OR PERHAPS FOR OTHER REASONS. THIS ARTICLE LOOKS AT THE ROLE OF STANDARDS IN SECURING GEOSPATIAL INFORMATION.

Internet and Web standards organizations play a key role in providing the infrastructure that ultimately enables content and service providers to control which individuals (or processes operating on their behalf) will have permission to read, write, create or delete information. This article describes activities in the Open Geospatial Consortium, Inc. (OGC®) that have focused on security of geospatial content and services.

The OGC's security focus

Within the OGC, the members have created three main activities that address security and related topics:

- The Geo Rights Management Domain Working Group (GeoRM DWG) has produced the Geospatial Digital Rights Management Reference Model (Abstract Specification Topic 18), and a related GeoRM Common Standards Working Group is defining a standard to implement that reference model. The goal is to provide industry with a standards-based, automated system for implementing operating agreements. This system will enable broader distribution and licensed use of geodata while managing the rights of producers and users. Also, users need such a system if they are to have concrete terms-of-use that reduce their legal risks. Rights management and security are separate topics, but uses cases for security are often closely related to use cases for rights management services.
- The Security DWG is a forum for discussing topics related to authentication, access control and secure communication.
- The OGC GeoXACML Standards Working Group developed GeoXACML, which is based on the OASIS XACML standard. XACML (eXtensible Access Control Markup Language) was

developed by OASIS (the Organization for the Advancement of Structured Information Standards). This working group continues to coordinate OGC's work on GeoXACML with OASIS's work on XACML.

Also, in 2009 the OGC Board of Directors created the OGC Spatial Law and Policy Committee to provide an open forum for OGC members' legal and policy advisors to discuss the unique and increasingly critical legal and policy issues associated with spatial data and technology.

Security in OGC testbeds

Each year, the OGC organizes an OGC Web Services (OWS-*) testbed activity in which OGC standards are implemented, tested and improved, and in which candidate OGC standards are developed and tried in hands-on prototyping activities. These activities are based on a diverse set of sponsors' interoperability requirements expressed in use cases that derived from real-world scenarios. The OWS-3, OWS-4, OWS-6 and OWS-7 testbeds included security "threads", as described below.

OWS-3 (2005)

OWS-3 addressed "click-through" licensed use by a:

- Web Map Service (WMS)
- Web Feature Service (WFS)
- Web Portrayal Service (cascade of a WMS and WFS)
- GeoDRM license model for different types of users - anonymous / registered user

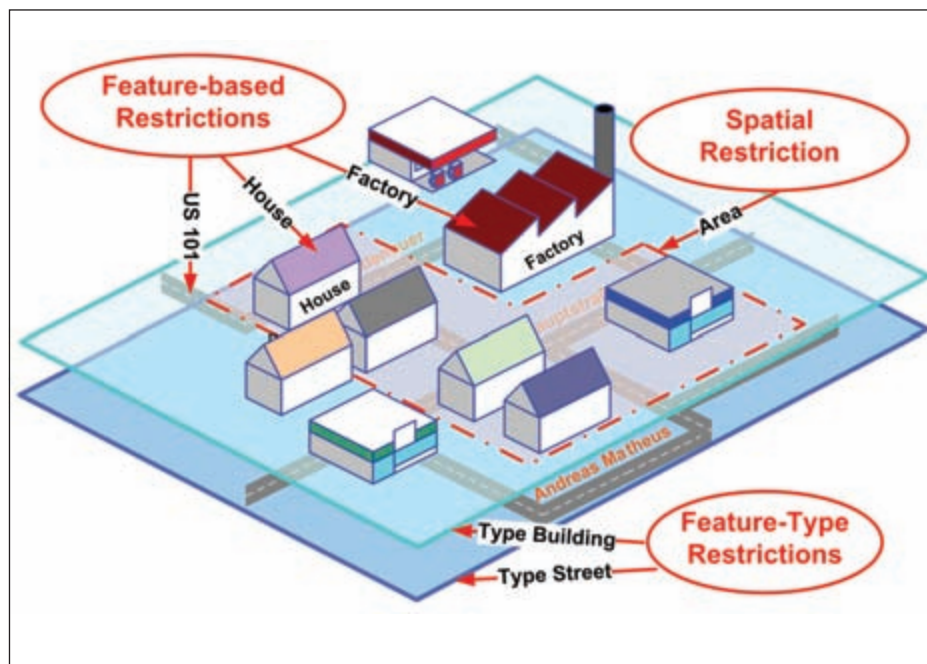
This early demonstration of secured implementations of OGC Web Services standards used WS-Security (Web Services Security), an extension to SOAP (originally defined as Simple Object Access Protocol) that allows applications to apply integrity and confidentiality but also to exchange security tokens, which is an OASIS protocol specification for exchanging structured information in the implementation of Web services in computer networks.

OWS-4 (2006)

OWS-4 included a dedicated thread for GeoDRM. This involved use of brokered / negotiated licenses for a service implementing the OGC Web Feature Service (WFS) Interface Standard.

OWS-6 (2008)

OWS-6 included security requirements in geoprocessing workflows, providing managed access to services that implement OWS standards and trusted communication between different security domains. It also included GeoXACML-based protection of an implementation of the OGC Web Map Tiling Service (WMTS) Interface Standard and the OGC Web Feature Service (WFS) Interface



Ideally there would be a model for each community of interest that is then applied at a local or organisational level. This is a key objective of the emerging OGC Business Value Working Group.

Standard. (The WMTS Interface Standard is much like the OGC's popular Web Map Server (WMS) Interface Standard, but it enables better server performance in applications that involve many simultaneous requests.) OWS-6 also looked at security in the OGC Sensor Web Enablement (SWE) activity.

OWS-7 (2009 -2010)

OWS-7 addressed the secure interconnection of OGC Web Services within the SWIM System: the System Wide Information Management System of the FAA (Federal Administration of Aviation in the US). (See the recently released OGC Engineering Report "OWS-7 Secure interconnection of OGC Web Services with SWIM".)

Participants in these testbeds offered the following general guidelines:

- Use SOAP-based communication for service interfaces.
- Secure communication for workflow services by leveraging WS-Security from OASIS. This includes use of XML (eXtensible Markup Language) DSig (an XML syntax for digital signatures) and XML Encryption by W3C.
- For access control use GeoXACML.

It is important to note, however, that these guidelines, particularly the SOAP guideline, do not necessarily represent the general consensus in the OGC. OWS-* testbeds and other OGC interoperability initiatives such as interoperability experiments (see below) and pilot projects yield "engineering reports" that may be offered to the OGC Technical Committee for review and possible approval as draft standards, best practices or discussion papers.

Authentication Interoperability Experiment

In addition to the OWS testbed activities, the OGC provides "interoperability experiments." These are brief, low-overhead, unfunded, formally structured and approved initiatives led and executed by OGC members to achieve specific technical objectives that further OGC technical interoperability objectives.

The OGC Authentication Interoperability Experiment recently completed, tested standard ways of transferring authentication information between OGC clients and OGC services by leveraging mechanisms already existing in the Web's transport protocol (HTTP and SOAP). HTTP Authentication and SAML (Security Assertion Markup Language) mechanisms were tested, the latter including a Shibboleth implementation (see below).

An important product of this OGC Authentication Interoperability Experiment will be a public engineering report (to be posted on <http://www.opengeospatial.org/standards/paper>) that documents standard ways of performing authentication for OGC services.

Shibboleth: Security of federated systems requires interoperability

One important component of the OGC Authentication Interoperability Experiment was an investigation into an activity referred to as "Shibboleth Access Management Federations and Secure SDI." This has been funded by ESDIN (European Spatial Data Infrastructure with a best practice Network), a project supported by the EU eContentplus programme and coordinated by EuroGeographics. ESDIN Work Package 4 (WP4), "Data Access and Licensing Policy,"



Securing information about buildings and locations during major incidents, such as a fire at a major airport, while still providing the information needed to respond to an incident, requires automated levels of access and authentication.

addresses business model, pricing, and licensing models, and this includes issues such as: protection of intellectual property rights (IPR), security, access management, and privacy. Part of WP4 focuses on establishing a federation using Shibboleth, an open source package released by the Internet2 consortium. It implements SAML and thereby supports Web "Single Sign On" across administrative boundaries. Shibboleth based federations (predominantly in the academic sector) are being used by millions of users worldwide.

Also supported by ESDIN is the AGILE/EuroSDR/OGC "European Persistent Geospatial Testbed for Research and Teaching (PTB)". The PTB is currently using technology developed in the Shibboleth activity along with a number of European National Mapping and Cadastral Agencies (NMCAs). Participants in the PTB include EDINA, University of Edinburgh; FIUGINET (Finnish Universities Geoinformatics Network), CSC — IT Center for Science Ltd; Technical University of Dresden; and the Centre for Geospatial Science, University of Nottingham. On May 11, 2010, there was a pre-conference Persistent Test Bed workshop in association with AGILE 2010.

Most of the security use cases explored in the OGC activities described so far in this article involve "distributed systems" as opposed to "federated distributed systems". In a federated system, authenticated users from one community can be trusted and considered authenticated by another community without the second community having to maintain the authentication information (username and password, typically). In contrast, in a simple distributed system each transaction must be independently authorized and secured. Federated security is new to the geospatial domain.

Federated security typically does not use SOAP as a protocol between an OGC client and a service, but instead uses HTTPS and cookies. (Hypertext Transfer Protocol Secure (HTTPS) is defined in the World Wide Web Consortium [W3C] RFC 2818 and is a combination of HTTP with the widely used SSL/TLS protocol to provide encryption and secure identification of the server. An HTTP cookie, defined in W3C RFC 2109, is a small piece of text that Web applications can store in a user's Web browser.) HTTPS and cookies are essential parts of the Web services programming approach called REST (Representational State Transfer), which is an alternative to the SOAP approach. A main advantage of REST is interoperability, because virtually all Web clients and servers use the HTTP "stack" of standards, whereas SOAP can use any of several standards that are not always interoperable. REST, therefore, is a good way to provide basic capabilities inside a Web Browser. In the geospatial domain,

REST allows developers to use OGC Web Services interfaces and Web-based clients such as Google Maps and OpenLayers without changes.

The ESDIN Shibboleth effort, led by EDINA National Datacentre, was undertaken in part in response to the Commission's request to test practical existing solutions in eContentplus funded projects. With Shibboleth, organizations can exchange user information and make security assertions by obeying privacy policies. The ESDIN Shibboleth effort implements Shibboleth and the closely related Security Assertion Markup Language (SAML), and also the widely used OGC Web Map Service (WMS) Interface Standard. One of the most important outcomes of this effort is that no changes were required to Shibboleth or the current WMS standard.

To take this work forward, in cooperation with the OGC, the ESDIN project intends holding an ESDIN Shibboleth Authentication PlugFest in early November 2010. During the PlugFest, participating GIS vendors will gain access to the ESDIN Federation and have the opportunity to

demonstrate how their client software is capable of undergoing the Shibboleth/SAML interactions necessary to allow secure access to OGC Web Services in a Shibboleth Federation. More information about the Plugfest will be available shortly on the OGC website and through OGC and other relevant mailing lists.

What's the significance?

The Interoperability Experiment and the ESDIN work program described above demonstrate how a fundamental Spatial Data Infrastructure (SDI) requirement can be met using commonly used standards. The ESDIN consortium is comprised mainly of National



Mapping and Cadastre Agencies (NMCAs), including at this time KMS (Denmark), Kadaster (Netherlands), Lantmateriet (Sweden) and FOMI (Hungary). An ESDIN web browser based client using OpenLayers is currently under development that provides access to the Shibboleth (SAML) protected OGC Web Services of these NMCAs.

Access management federations provide a practical organisational model for operational SDIs, and Shibboleth, which supports such federations, provides a production strength security environment for large networks of organisations using OGC Web Services.

Part of the reason for setting up the ESDIN project was to assist European NMCAs in their preparation for implementation of the INSPIRE Directive. The ESDIN Federation provides a practical solution for how organisations with INSPIRE type framework agreements can be implemented. In this case, it could be any EU government agency with legitimate access to a federation of European NMCAs providing INSPIRE View and Download Services.

Potential future work items

Among the items that require further standardization work in the OGC are:

- Authentication
- Bootstrapping for secured OGC Web Services
- XACML Profile for OGC Web Services

While SAML provides a mechanism for making authentication and authorization assertions and a mechanism for conveying them, XACML provides the language that defines the rules needed to make the necessary authorization decisions. The OGC GeoXACML Standards Working Group is looking at ways to ensure 100% interoperability using GeoXACML to protect geospatial Web services, including services that implement OGC Web Services standards. The OGC group continues to communicate with OASIS XACML Working Group to ensure that geo-specific use cases are included in that group's work.

Links - (in order of appearance in the article)

GeoRM DWG:

www.opengeospatial.org/projects/groups/geormwg

Security DWG:

www.opengeospatial.org/projects/groups/securitywg

GeoXACML Standards Working Group:

www.opengeospatial.org/projects/groups/geoxacmlswg

OGC Spatial Law and Policy Committee:

www.opengeospatial.org/pressroom/pressreleases/964

Web Map Service (WMS):

www.opengeospatial.org/standards/wms

Web Feature Service (WFS):

www.opengeospatial.org/standards/wfs

OWS-6 Security Engineering Report:

portal.opengeospatial.org/files/?artifact_id=35461

Web Map Tiling Service (WMTS) Interface Standard:

www.opengeospatial.org/standards/wmts

Sensor Web Enablement (SWE) activity:

portal.opengeospatial.org/files/?artifact_id=34273

Authentication Interoperability Experiment:

www.opengeospatial.org/projects/initiatives/authie

Security Assertion Markup Language: en.wikipedia.org/wiki/SAML

European Persistent Geospatial Testbed for Research and Teaching

(PTB): sdi-testbed.eu

Persistent Test Bed Workshop:

agile2010.dsi.uminho.pt/workshops.html

REST (Representational State Transfer):

www.ics.uci.edu/~fielding/talks/webarch_9805/

Article by *Andreas Matheus*, *Secure Dimensions GmbH*

(andreas.matheus@secure-dimensions.de), *Chris Higgins*, *EDINA*

(chris.higgins@ed.ac.uk), and *Steven Ramage*, *Executive Director*,

Marketing and Communications, *Open Geospatial Consortium (OGC)*

(sramage@opengeospatial.org).

Geospatial Data and Geovisualization: Environment, Security, and Society

ASPRS/CaGIS 2010 Specialty Conference

in conjunction with

a special joint symposium of

ISPRS Technical Commission IV and AutoCarto 2010

Orlando, Florida, USA November 15–19, 2010

www.asprs.org/orlando2010

Sponsored by

In Cooperation with

