A Shibboleth Service Provider for OGC Web Map Services

Andreas Matheus
Universitaet der Bundeswehr Muenchen
D-85579 Neubiberg, Germany
andreas.matheus@unibw.de

Chris Higgins
University of Edinburgh
Edinburgh, UK
chris.higgins@ed.ac.uk

ABSTRACT

Geospatial data is an important source of information for many different user communities. One of the largest communities is science and education: in the UK, approx. 8 million users are sharing resources and services for collaborative projects. The shared use of resources is organized as a service and identity federation using the Shibboleth implementation of the Security Assertion Markup Language (SAML). This enables the establishment of trust relationships amongst partners of the federation and the secure protection of resources and services from unauthorized use. Unfortunately, the federations existing in the UK, US and Australia do not currently provide access to geospatial web services. Specifically, they do not provide access to Geo Web Services as standardized by the Open Geospatial Consortium (OGC). One of the reasons is that the OGC Web Services standards are not concerned with security. It is therefore extremely difficult to ensure interoperability when it comes to dealing with protected OGC Web Services as required, for example, within the science and education community.

The JISC funded a project called SEE-GEO (SEcurE access to GEOspatial services) to find solutions for integrating OGC Web Services with the Shibboleth based UK Access Management Federation. This paper will describe the challenge and the novel solution of the SEE-GEO project to protect and securely integrate an OGC Web Map Service into a Shibboleth federation as a result of collaboration between academia and commercial participants.

Categories and Subject Descriptors

D.4.6 [**Security and Protection**]: Access controls; D.4.6 [**Security and Protection**]: Authentication

General Terms

Reliability, Security, Standardization

CCS'09, November 9-13, 2009, Chicago, IL ,USA.

Keywords

GeoXACML, XACML, SAML, SDI, OGC, Shibboleth, Internet2, Access Management, Web Services

1. MOTIVATION

In the United Kingdom, the Joint Information Systems Committee (JISC) (see [7]) has "led the policy initiative in the UK to deploy Shibboleth as the next generation access management technology for authentication and authorization across the science and education sector."[1] Effective as of August 1st this year, most Universities in the UK stopped using the Athens system for accessing online services and switched to Shibboleth (see [6]). In 2006, the JISC funded the EDINA National Datacentre, based at the University of Edinburgh, to commence leading work on the SEcurE access to GEOspatial services (SEE-GEO) project. The purpose of SEE-GEO was to investigate the means of making geospatial data securely available within the context of Grid technology and standards from the Open Geospatial Consortium (OGC) (see [11]).

This paper may be considered as an engineering report covering some of the results from the SEE-GEO work undertaken to address the following two key challenges:

- How can access to an OGC Web Services (see [14]) such as a Web Map Service (WMS) (see [12]) or a Web Coverage Service (WCS) (see [13]) be secured in terms of Access Control, and
- How can the protected OGC Web Service be integrated into an existing Shibboleth authentication framework leveraging the currently existing OGC Web Service interfaces.

2. THE SEE-GEO CHALLENGE

Shibboleth is typically used to protect web resources accessed from web browsers. It is important to understand that, in terms of the interactions taking place, that these differ from the interactions that typically take place between an OGC Web Service client and an OGC Web Service. Therefore, the standard Internet2 implementation cannot be used and the service provider has to be designed and implemented from scratch, according to the SAML interface specification. For example, in a typical Shibboleth exchange, if an unknown user wants to access a "Shibbolized" web resource, the request is redirected and the user is required to authenticate. After a successful login, the user's web browser is

redirected back to the protected resource. In order to support Single-Sign-On, the service provider and the identity provider maintain a session which has associated a security context that includes information about the user. The use of an OGC Web Service is such that the client calls the GetCapabilities operation of the service and the service expects a response back. This can either be the actual capabilities document or an error report, both formatted in XML. This coarse description raises a number of important questions:

1. How can the Shibboleth login sequence be initiated by the client and what information does the client need to have in order to do so? The concrete requirement for the solution was that it shall fit seamlessly into the existing Shibboleth Management Federation for the UK academic institutions. This creates further requirements in terms of the version of SAML. As the Shibboleth network has version 1.3 IdPs, support for SAML2 was available. This is important, as SAML2 provides an SSO Browser Profile based on SAML artifacts that is not available in SAML1.

2. How can the client establish a security context with the service leveraging the OGC Web Services interface without modifications? In particular, this means that we have to find a solution to protect the WMS and integrate it into the Shibboleth Single-Sign-On network based on the WMS version 1.1.x interface.

3. How can access control be established? As the existing WMS had endpoints exposed for use within an existing infrastructure, it was a requirement to provide an architecture that supports access control around existing network endpoints without causing any interference with current operation. Additional requirements for access control originated from the use case scenarios. For example, it was mandatory to control access to the WMS based on different types of information, eg, the area of interest for which the operator is requesting a map, the nationality of the operator and the applied styling. Also, it should be possible to exchange access rights in an interoperable format to guarantee harmonization across jurisdictions.

4. The solution shall support existing OGC Web Services such a WMS 1.0 or a WMS 1.3 and the client shall be a browser based application.

3. A SHIBBOLETH SERVICE PROVIDER FOR OGC WEB MAP SERVICES

In general, the architecture is a Service Oriented Architecture, where the services and the client are distributed over an insecure network, ie, the Internet. It can be separated into three different domains: The Identity Service Provider Site, the Service Provider Site and the Client Site, as indicated by the pink dashed line in the architecture figure (see **??**). For this project, we assume static trust relationships between the Service Provider(s) and the Identity Provider(s) established by an exchange of X.509 certificates. According to the SAML specification, this is a valid assumption.

The software components can be separated into regular Shibboleth software for the Identity Provider as downloaded from the internet2 site, and the Service Provider software components that were implemented for the SEE-GEO project:

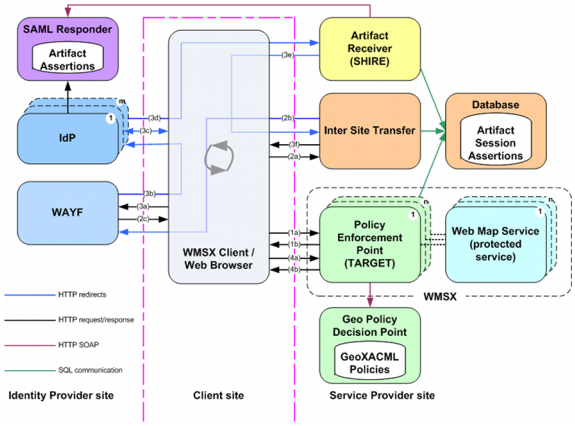

Figure 1: Architecture and sequence of interactions for a web browser based WMSX client

The SAML Responder is an optional service that can be part of the IdP. It manages the association of user assertions (based on the login) and a SAML artefact. This allows the Artefact Receiver service component of the Service Provider to request the user SAML assertions associated with a particular SAML artefact. This Service is not directly involved in the sequence of interactions concerning the web browser. A so called back-channel communication with SOAP is used.

The Protected Resource Service is the component that checks for valid user assertions before granting access to the protected web resource. In the case where the user has not authenticated or an earlier established session has expired, the Protected Resource Service initiates a redirect to the Inter-Site Transfer Service indicating itself as the final target.

The Inter-Site Transfer Service is responsible for forwarding the redirect to one of the trusted WAYFs and indicating the Artefact Receiver Service as the legitimate receiver of the SAML artefact. The Service indicates that by using the parameter SHIRE= For our project, we only have one WAYF, so the functionality for the standard Shibboleth interactions are quite simple. However, the Inter-Site transfer Service plays a more important role for protecting a WMS.

The Artefact Receiver Service is mainly responsible for accepting redirects from the Identity Provider (IdP) and for the Browser SSO Profile requests for user assertions, associated with the received SAML artefact. This is achieved using a SOAP enabled back channel communication with mutual HTTPS or one-way HTTPS plus Digital Encryption on the request message.

4. PROOF OF CONCEPT IMPLEMENTATION AND DEMO

The cross border use case, as described in [4] requires that a German and a Dutch rescue center share topographic maps for disaster management, affecting both countries. This requires that a German operator can see Dutch terrain maps and that the Dutch operator can see German maps - under certain constraints. In order to make the topographic maps of the other and the home country look the same to the operators, the Web Map Service provides user specific styling: Dutch and German styling is available. This ensures that for example:

Table 1: Use Case Scenarios

Scenario	Description
#1	A German operator can apply German styling to maps showing German terrain only
#2	A Dutch operator can apply Dutch styling to maps showing Dutch terrain only
#3	A German operator cannot access Dutch terrain maps only - No cross-border operations map
#4	A Dutch operator cannot access German terrain maps only - No cross-border operations map
#5	A Dutch operator can never apply German styling, regardless to the area of interest for which a map is requested
#6	A German operator can never apply Dutch styling, regardless to the area of interest for which a map is requested
#7	A German operator can apply German styling to maps showing Dutch and German terrain - Cross border operations map
#8	A Dutch operator can apply Dutch styling to maps showing German and Dutch terrain - Cross border operations map

The access restrictions that exist for the Dutch and German operator are based on the choosen styling and on the area of interest for which a map is requested. Table 1 provides a compact view on all scenarios upon which access restrictions are based on.

By using the facade architecture pattern for the service side, we were able to deploy a proxy service – the Policy Enforcement Point (PEP) – at the SP site that interacts on behalf of the unprotected WMS at domains of AM Consult (http://www.geoxacml.org) and the University of Edinburgh (dlib-mumra.ucs.ed.ac.u). In order to guarantee that no client can bypass the PEP, we control network traffic to the unprotected WMS through a firewall that accepts external connections only from trusted Service Providers to the PEP. We enforce Access Control in the PEP by requiring the WMS client user to authenticate via the Shibboleth Identity Federation providing a Security Assertion Markup Language (SAML) (see [10]) identity token or assertions to the SP. Based on the role attribute of the user, a Geospatial eXtensible Access Control Markup Language (GeoXACML) (see [9]) policy is enforces the users access rights. In order to demonstrate the proof of concept implementation, we have created a GeoXACML policy according to the so called Cross Border Use Case that was provided to the AGILE/EuroSDR/OGC initiative Persistent European Geospatial Testbed for Research and Teaching (PTB) by the University of the Bundeswehr (see [2]).

Please note that an online demonstration is available but at the time of writing the authors do not have permission to make the URLs publicly available.

5. CONCLUSION AND FUTURE WORK

In order to protect a WMS as described way and to integrate it into the Shibboleth SSO Network, no changes to the existing OGC Web Map Service specification is required. However, the protection and the integration into Shibboleth require additional functionality on the WMS service and in particular on the WMS client side. This additional client functionality mainly incorporates the processing of a particular WMS Exception that contains certain information such as the redirect URL and a session specific GetCapabilities URL.

We see future work in the area of investigating how this solution can be applied for Desktop Clients. In particular we see the need to evaluate the use of a SOAP based interface that is based on the Enhanced Client Profile (ECP).

Future work in terms of standardization potentially exists to ensure an interoperable use of the illustrated solution.

6. REFERENCES

[1] Joint information systems committee (jisc) sdss access management group.

[2] Persistent european geospatial testbed for research and teaching.

[3] Uk access management federation.

[4] S. S. Andreas Matheus. Unified portrayal of geospatial cross-border information, 2007.

[5] S. Cantor. Shibboleth architecture, protocols and profiles. Technical report, Ohio State University, September 2005.

[6] Internet2. Shibboleth homepage.

[7] JISC. Joint information systems committee.

[8] JISC. Secure access to geospatial services (see-geo).

[9] A. Matheus. Geospatial extensible access control markup language (geoxacml), version 1.0. Implementation specification, Open Geospatial Consortium, Inc., http://portal.opengeospatial.org/files/?artifact_id=25218, February 2008.

[10] OASIS. Profiles for the oasis security assertion markup language (saml) v2.0. Specification, OASIS, http://www.oasis-open.org/specs/index.php#samlv2.0, March 2005.

[11] OGC. Open geospatial consortium, inc.

[12] OGC. Web map service implementation specification, version: 1.1.1. Implementation specification, Open Geospatial Consortium Inc. (OGC), http://www.opengeospatial.org/standards/wms, January 2002.

[13] OGC. Web coverage service (wcs), version 1.0.0 (corrigendum). Implementation specification, Open Geospatial Consortium Inc. (OGC), http://www.opengeospatial.org/standards/wcs, October 2005.

[14] A. Whiteside. Opengis web service common implementation specification. Implementation specification, Open Geospatial Consortium Inc., http://www.opengeospatial.org/standards/common, 2005.

Acknowledgment

The authors like to thank the Joint Information Systems Committee (JISC) (see [7]) in the United Kingdom for funding the research project SEE-GEO (see [8]).