

Project Acronym: WSTIERIA  
 Version: 2  
 Contact: Fiona Culloch  
 Date: 23/02/10



## Project Plan

Project Information			
<b>Project Acronym</b>	WSTIERIA		
<b>Project Title</b>	Web Services Tiered Internet Authorisation		
<b>Start Date</b>	04/01/2010	<b>End Date</b>	31/12/2010
<b>Lead Institution</b>	EDINA National Data Centre		
<b>Project Director</b>	Peter Burnhill		
<b>Project Manager &amp; contact details</b>	Fiona Culloch, Tel: (0131) 651 7721 Email: <a href="mailto:fiona.culloch@btinternet.com">fiona.culloch@btinternet.com</a>		
<b>Partner Institutions</b>	-----		
<b>Project Web URL</b>	<a href="http://edina.ac.uk/projects/wstieria_summary.html">http://edina.ac.uk/projects/wstieria_summary.html</a>		
<b>Programme Name (and number)</b>	<i>Access and Identity Management</i>		
<b>Programme Manager</b>	Christopher Brown		

Document Name			
<b>Document Title</b>	Project Plan		
<b>Reporting Period</b>			
<b>Author(s) &amp; project role</b>	Fiona Culloch, Project Manager		
<b>Date</b>	19/02/2010	<b>Filename</b>	
<b>URL</b>			
<b>Access</b>	<input checked="" type="checkbox"/> Project and JISC internal		<input type="checkbox"/> General dissemination

Document History		
Version	Date	Comments
2	23/02/10	Incorporate feedback from JISC Programme Manager
1	19/02/10	First external release





## JISC Project Plan

### *Overview of Project*

#### **1. Background**

This project emerged from the JISC-funded SEE-GEO<sup>1</sup> project, which developed a viable technique for controlling access to REST-style web services using one of the standard SAML federated access management profiles. Ordinarily, federated access management software cannot be used to protect web services because, unlike a browser accessing a web site, a given web service client application may not be designed to support user interaction (to type a username and password into an HTML form or select an identity provider). Additionally, many interesting clients, particularly some specialised desktop applications, cannot handle federated access protocols because they do not support either SSL/TLS or some features of HTTP, commonly redirection or cookies. They may also be unable to render HTML; usually they process application-specific XML documents instead.

The technique developed by SEE-GEO is for access to the web service to be controlled, not by standard federated access management software but by a “façade” web service, which checks for the presence of an access token in requested URLs. If a valid token is present, the request is forwarded to the protected service behind the façade and the response returned to the client. The client is prevented from directly accessing the underlying service by a firewall (or equivalent) configured to accept requests from the façade service only. A valid token is obtained by a prior HTTP request to a URL associated with, but distinct from, the web service itself. This other URL initiates a standard SAML flow, which can if necessary be processed separately from the client, without any constraints related to redirection or cookies, for example by starting up a full web browser. Once authorised in that context, the user has a valid token that will be accepted by the façade and can be used by even the most limited client software.

An evaluation report by Chad La Joie of the Shibboleth Core Team, written after completion of the SEE-GEO project in 2008, recommended that:

- The custom SAML Service Provider (SP) code built in to the SEE-GEO façade software, which was derived from an earlier phase of work where SAML support was directly integrated into the underlying web service rather than split out into a façade, should be replaced by standard SP software, specifically Shibboleth.
- Because the HTTP Redirect and Artifact SAML bindings used in the SEE-GEO work have some deployment issues (a SAML authentication request encoded within a URL may exceed a web server’s maximum URL length, and the Artifact binding requires a back-channel between Identity Provider and Service Provider that experience shows many deployers have difficulty setting up), investigate using the HTTP POST binding instead.
- One or two developers should spend part of their time working directly on EDINA web services and part with the JISC Expert Group in Identity Management (SDSS, also based at EDINA), to speed progress by combining application and UK federation expertise.

These recommendations form the background to the “façade software” work package of this project. Motivation was provided by EDINA’s production web services. At present, some of these which might

---

<sup>1</sup> <http://edina.ac.uk/projects/seesaw/seegeo/>

be of general use to the community are restricted to use within EDINA. Since the launch of the UK federation in 2006, EDINA has wanted to make these web services generally available to users authenticated via the federation but has been prevented for the reasons outlined at the beginning of this section. There is therefore an internal need for this functionality. Any organisation wanting to provide a web service to UK HE/FE that requires user authentication will have a similar requirement, since federated access is now the standard in the sector, so the need was seen to be widespread.

Independently from this work at EDINA, the Shibboleth Core Team has been working with developers at the University of Chicago to extend Shibboleth itself to support web services directly. This has recently been achieved in the context of portal applications (specifically uPortal).

In the scheme adopted, the user first uses a browser in the normal way to log in to the portal web application, which is protected by a Shibboleth SP. The portal application can then invoke web services. These web services may themselves be protected by Shibboleth SP software. Instead of the usual browser-based SAML flows, the web service SP interacts with its client (the portal application) using the SAML Enhanced Client or Proxy (ECP) profile, which does not assume the presence of a browser. The client invokes the web service via a library that can:

- accept ECP authentication requests from the web service SP;
- forward these to the identity provider originally used to log in to the containing portal SP, along with a reference to the user in the form of the SAML authentication assertion originally provided to the client SP during the “normal” login;
- send back the resulting authentication response.

This process is designed to be chained, supporting n-tier applications in which one web service invokes another, with the “deepest” one still being able to pass authentication requests back upstream to the user’s identity provider and receive authentication responses.

The “Shibboleth n-tier integration” work package in this project is intended to allow us to become familiar with this new approach by deploying and experimenting with it, using an EDINA web service as a test bed and potentially providing useful feedback to the developers. There is an obvious need for developers in the UK to become familiar with this emerging technology, to act as a focus for dissemination and support as it is adopted more widely.

Because it has no standard, secure way to pass on a reference to the user from one web service to another, the façade method is less powerful than the native Shibboleth approach, although it may be possible to combine the two. Otherwise the façade method is restricted to one-tier applications. Nevertheless it is still being taken forward because:

- It does not require the use of a particular client library to invoke the web services. Although libraries are already available for Java and some other languages, this may still be a problem in some deployment environments.
- Since no special library is required, fewer modifications are needed to the client code. In cases where some user intervention is acceptable at run time (to copy a token from a separate browser session), a completely unmodified client can even be used. This is important with commercial desktop clients for which source code is not available.
- The native Shibboleth method requires SAML 2.0 ECP support in the user’s identity provider. As of the end of December 2009, only just over 20% of deployed UK federation identity providers were configured with support for SAML 2.0.
- The façade provides a convenient place to implement and maintain arbitrary authorisation code separately from the underlying web service. A Shibboleth SP allows for simple authorisation logic to be expressed declaratively in its configuration language, but if more

complicated authorisation is required presumes that the application being protected is Shibboleth-aware and will make the decision itself, based on the attribute data provided to it. The façade allows a web service implementation to remain unaware of authorisation issues.

- The façade method will work with any authentication mechanism, not just Shibboleth, without modifying the code of the protected web service.
- It is conceptually similar in some ways to the OAuth WRAP proposal that has been contributed to the IETF OAuth working group for standardisation, in which an extended HTTP Authorization request header contains a token instead of the URL. It may therefore offer a future migration path to integration with wider standards.

Because the previous SEE-GEO work was done in the context of Open Geospatial Consortium (OGC) web services, this project will continue to use OGC web services as test cases and examples, and to ensure that development is grounded in concrete user requirements outside the control of the project team. However, both the façade method and the Shibboleth native method are generic. Mostly, neither need understand the specifics of OGC services, which are mainly related to the application-specific XML content involved. In both cases this application-layer data can usually be passed through completely unmodified.

## 2. Aims and Objectives

The aim of the project is to produce software and documentation that will allow developers of web services to make use of the UK Access Management Federation for Education and Research to authenticate end users and obtain attributes about them for authorisation purposes. This software should not require modification of the web service being protected but may require some modifications to client software.

## 3. Overall Approach

Initially the team will investigate the previous work by the Shibboleth Core Team and EDINA (supported by consultancy from Chad La Joie of the Shibboleth Core Team and key people from the JISC-funded EDINA SEE-GEO project) and develop the middleware outputs. The project team will then liaise with EDINA application development teams to develop an example use case and in parallel identify possible future external partners.

The critical success factor is the identification of external organisation(s) and individuals willing to cooperate with the project and act as test web service clients. Although EDINA uses a significant number of web services internally, these are protected by IP-address checking only, with user authentication performed beforehand by a trusted web application front end. The web services are not externally accessible and trust the front end to act only on behalf of authorised users. To provide a realistic environment, one or more of these web services must be made externally accessible and provided with suitable authorisation decision-making code.

## 4. Project Outputs

The project will have the following tangible outputs:

1. Façade software that web service developers can deploy in front of their own services to handle federated access management
2. A demonstration OGC web service using this software, accessible via the standard UK federation authentication mechanisms
3. Experimental (pre-demonstrator stage) modifications to chosen EDINA web services (likely to be OGC web services) to act as test use cases for prototype n-tier Shibboleth features

4. A draft and then final report documenting the other deliverables and the project's experiences
5. A six-month progress report and a project completion report.

The more intangible outputs should include:

1. Building enough hands-on understanding of the native Shibboleth approach to be able to support others setting off down that road.
2. Finding out more about external developments in this area.

## 5. Project Outcomes

The following project outcomes are desired:

1. The increasing availability of education-focused, production web services supporting federated authentication.
2. Wider access to web services that are presently kept hidden behind firewalls because they require user authentication that is not supported by presently deployed federated access management software.
3. In consequence, the appearance over time of richer, more powerful applications for end users in all areas of education due to the greater availability of back-end "component" web services that can be simply combined rather than re-invented by application developers.

## 6. Stakeholder Analysis

Stakeholder	Interest / stake	Importance
EDINA Geospatial Team	Transitioning from project to production	High
MIMAS	Service interoperability	High
UK Access Management Federation	Increasing the domain of applicability of federated access management	Medium
Shibboleth Core Team	Use cases	Medium

## 7. Risk Analysis

Risk	Probability (1-5)	Severity (1-5)	Score (P x S)	Action to Prevent/Manage Risk
Staffing	2	3	6	Choice of demonstrator examples has been left as open as possible to allow maximum flexibility in staff assignment
Organisational: Identifying user requirements well requires working with users <b>outside</b> EDINA, because internally used web services only realistically need IP-address checking	4	4	16	Prioritise identification of external organisations and individuals willing to work with the project.
Technical: Potential conflict between geo team preference for Java in code	3	2	6	Stress implementation at server side is hidden from app code behind a URL/web service

they rely on and/or maintain vs. developer skill set (perl, C++)				interface. At client, multiple language bindings will eventually be required (and hiding behind URL is also possible).
External suppliers				N/A
Legal: An Ordnance Survey licence condition requires 20min session timeouts. Caused problems for a previous web services trial.	5	1	5	Unlikely to be addressed within the context of this project, but being taken forward elsewhere. Should not seriously affect demonstration use. Announced changes in government policy on use of OS data may anyway negate this risk for some services.

## 8. Standards

Name of standard or specification	Version	Notes
HTTP	1.1	
SAML	1 and 2	Native Shibboleth n-tier support requires SAML 2.0. The façade approach should work with either. The Shibboleth 1.x software releases (IdP and SP) do not support SAML 2.0, but this is becoming less relevant over time, as take-up of Shibboleth 2.x increases and 1.x heads towards end-of-life in June 2010.
OGC WMS	1.1.1	

## 9. Technical Development

The intention is to follow a “release early, release often” model to be able to adapt flexibly to changing requirements identified by external testing.

## 10. Intellectual Property Rights

Project IPR will be owned by EDINA. It is not currently anticipated that the project outputs will include third-party components except by reference (e.g., libraries downloadable from public repositories).

## *Project Resources*

### 11. Project Partners

N/A

### 12. Project Management

The project manager has overall responsibility, supported by a senior project advisor, and will also be the middleware developer (façade software, Shibboleth n-tier experimentation).

The applications liaison will report to the project manager and has responsibility for:

- identifying external organisations and individuals willing to cooperate with the project (as web service clients)

Project Acronym: WSTIERIA  
 Version: 2  
 Contact: Fiona Culloch  
 Date: 23/02/10

- identifying use cases
- direct supervision of progress by an application developer

The application developer will work directly with the project manager (in the role of middleware developer), while also reporting to the application liaison.

Team members:

- Project Manager (10% of time) and middleware developer:  
 Fiona Culloch, Tel: (0131) 651 7721, Email: [fiona.culloch@btinternet.com](mailto:fiona.culloch@btinternet.com)
- Project Advisor:  
 Sandy Shaw, Tel: (0131) 650 4988, Email: [s.shaw@ed.ac.uk](mailto:s.shaw@ed.ac.uk)
- Application liaison:  
 Chris Higgins, Tel: (0131) 651 1440, Email: [erpl70@holyrood.ed.ac.uk](mailto:erpl70@holyrood.ed.ac.uk)
- Application developer:  
 To be identified when demonstration use case is chosen

No training requirements have been identified at this time.

### 13. Programme Support

N/A

### 14. Budget

See Appendix A. Budget is unchanged from the agreed proposal.

### *Detailed Project Planning*

### 15. Workpackages

See Appendix B.

### 16. Evaluation Plan

Timing	Factor to Evaluate	Questions to Address	Method(s)	Measure of Success
10/10 on	Deployability	Do project outputs get applied to real use cases?	Yes/No	Deployment by EDINA on externally visible production services
04/10 on	User acceptability	Do project outputs get applied by external entities?	Yes/No	Production use of façade software package outside EDINA

### 17. Quality Plan

Output	Façade Software				
	Quality criteria	QA method(s)	Evidence of compliance	Quality responsibilities	Quality tools (if applicable)
04/10-		External code review outside	Subsequent version(s)	FC	N/A

		direct project team	incorporating recommended changes		
--	--	---------------------	-----------------------------------	--	--

Demonstration OGC Web Service					
Output	Quality criteria	QA method(s)	Evidence of compliance	Quality responsibilities	Quality tools (if applicable)
Timing	Available on demand	External testing	Available on-demand to external testers	FC (façade), CH (underlying OGC service)	N/A

Experimental N-Tier Setup					
Output	Quality criteria	QA method(s)	Evidence of compliance	Quality responsibilities	Quality tools (if applicable)
Timing	Very low; doesn't crash on internal demos		Successful Internal demos	FC	N/A

Project Reports					
Output	Quality criteria	QA method(s)	Evidence of compliance	Quality responsibilities	Quality tools (if applicable)
Timing	Completeness, comprehensibility	Internal review during production	Reviewer comments incorporated in subsequent versions	FC, SS	N/A

## 18. Dissemination Plan

Timing	Dissemination Activity	Audience	Purpose	Key Message
03/10	Presentation to Security DWG at OGC TC meeting at ESA, Frascati, Italy	OGC members	Raise awareness of project aims, gain feedback on user requirements	Likely future availability of federated access to OGC web services
07/10-	Paper on project work and outcomes	Developers of web services targeted at HE/FE, particularly OGC web services	Inform audience of the existence of deployable techniques for federating web services	"You can do it now"

## 19. Exit and Sustainability Plans

Project Outputs	Action for Take-up & Embedding	Action for Exit
Façade software	Package published on project web site. If deployed by EDINA on production web services then package will be maintained, otherwise simply preserved for the required duration of the project web site.	(If not deployed) Preservation as described under "take-up"
Demo OGC web service	Publish links to demo on relevant mailing lists etc. If significant usage is seen then argue within EDINA for continuing maintenance, otherwise exit.	Silently take down
Experimental n-tier setup	Not intended to be externally visible. However, knowledge gained will be made available to the community via the report and through project staff contributions to relevant mailing lists.	Decommission system if convenient
Project report	Publish on web sites (project, JISC), inform potential readers via mailing lists (JISC-SHIBBOLETH et al)	N/A

The following project outputs may have potential to live on after the project ends:

Project Outputs	Why Sustainable	Scenarios for Taking Forward	Issues to Address
Façade software	Generally applicable software	1) If in production use by EDINA, continued maintenance as a normal operational activity. 2) Otherwise, exit (publish and preserve)	In 1), approach to integrating community feedback, patches: evolution to open-source project?

## Appendixes

### Appendix A. Project Budget

See separate file.

### Appendix B. Workpackages

See separate file.