WORKSHOP: Shibboleth Federations and Secure SDI: Outcomes and Demonstrations from the OGC Web Service Shibboleth Interoperability Experiment

Chris Higgins, IE Manager, EDINA National Datacentre, University of Edinburgh, Scotland

INSPIRE Conference 2011, Monday 27th June
# Workshop Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1600-1620</td>
<td>Introduction</td>
</tr>
<tr>
<td>1620-1640</td>
<td>Member States investigating use of Shibb for their NSDI’s</td>
</tr>
<tr>
<td>1640-1710</td>
<td>Demonstration of software working with the test Federation</td>
</tr>
<tr>
<td>1710-1730</td>
<td>Questions and concluding remarks</td>
</tr>
</tbody>
</table>
ESDIN Project

- Resourced EDINAs participation in OSI
- An eContentplus Best Practice Network project
- September 2008 to March 2011
- Coordinated by EuroGeographics
- **Key goal**: help member states prepare their data for INSPIRE Annex 1 spatial data themes and improve access
- Been taking forward as the European Location Framework
ESDIN project info (www.esdin.eu)

- Project partially funded by eContentplus programme
- Started in September 2008 and will run for 30 months until March 2011
- Coordinated by EuroGeographics with 20 project partners
EDINA

- A National Data Centre for Tertiary Education since 1995
  
  *to enhance the productivity of research, learning and teaching in UK higher and further education (mission statement)*

- Focus is on services but also undertake r&D

- Shibboleth used primarily in academic sector
  - [https://www.aai.dfn.de/links/](https://www.aai.dfn.de/links/)
  - [https://spaces.internet2.edu/display/SHIB/ShibbolethFederations](https://spaces.internet2.edu/display/SHIB/ShibbolethFederations)

- EDINA provides technical support in the operation of the UK Access Management Federation
  - Approx 8 million users
  - 837 Member Organisations (IdPs and SPs)
OGC Web Service Shibboleth Interoperability Experiment (OSI)

- OGC Interoperability Experiments are:
  - Simple, low overhead, means for OGC members to get together and advance specific technical objectives within the OGC baseline
  - Voluntary
  - Facilitated by OGC staff

- OSI Press release inviting participation 31st Aug 2010
- Technology Integration Experiment on 18th Nov 2010
- Draft version of the Engineering Report (OGC 11-019)
  - ER to be completed before September 2011 OGC Technical Committee meeting
So what’s the problem?

• Many of the most valuable SDI resources are protected
• These resources frequently in different admin domains
  – Example: Article 19 of the INSPIRE Directive “…Member States may limit public access…etc, etc”.
• No widely accept standard for securing these protected geospatial resources
  – Consequence: lots of point solutions
• Major interoperability barrier, eg, how can a X-Border application consume protected OWS while having to deal with multiple different access control mechanism?
  – Make everything open? or,
  – Access Management Federations (AMF’s)? or, …?
What can AMF’s do for us?

• Fundamental requirement: information on who is accessing your valuable resource = authentication
• An AMF allows secure sharing of authentication information across administrative domains
• Members of a federation form a circle of trust and agree to procedures to enable these cross domain interactions
• Allows **Single Sign On**
• My X-Border appl can now access a protected resource in country A, be challenged for credentials, I authenticate and get access if authorised. Now I can also access additional federation resources (if authorised) in country A, B, C, …, **without** needing to reauthenticate
One Way - Shibboleth

- Internet2 consortium
- Open source package for web **Single Sign On** across admin boundaries based on standards:
  - Security Assertion Markup Language (SAML)
- Organisations can exchange user information and make security assertions by obeying privacy policies
- Devolved authentication – maintain and leverage existing user management
- Enables finer grained authorisation through use of attributes
Why put effort into federated access control round OGC Web Services?

- Open geospatial interoperability standards underpin SDI
- OGC standards agnostic about security
- Lack of a genuinely interoperable security solution a major barrier in all sectors
- INSPIRE-like, the EU requested that the ESDIN project focus on testing practical existing solutions
  - Integrates with existing identity management systems
  - Possibility of reusing existing member state federations or leveraging expertise
What we set out to do in OSI

- Previous work by the same team had shown it was possible to protect WMS with Shibb so that:
  - No mods required to OGC interfaces
  - No mods required to main Shibb download
  - BUT mods required to OWS clients
- Provide OGC software producing community with means and opportunity of modifying OWS client software to be able to work with Shibboleth AMF’s
- Emphasis on *desktop* OWS client software
- Provide participants with the opportunity to demonstrate their software in action.
OSI - How

• Use the test ESDIN Federation to provide OSI participants with services to develop against

• Provide an open source reference implementation of a modified desktop client conformant with the SAML ECP Profile

• Provide some technical support, eg, with OpenLayers clients conformant with the Web Browser SSO Profile

• Regular telcons

• OSI Technology Integration Experiment event
OSI - Who

- 36 individuals registered Shibb OGC portal site
- EDINA, Snowflake, Cadcorp, Envitia, con terra/ESRI, Joint Research Centre all modified their OWS client software or open source
- Federal Agency for Cartography and Geodesy (BKG) contributed another test Shibb federation they have been using for similar purposes
<table>
<thead>
<tr>
<th>Type of Client</th>
<th>Organisation Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EDINA (open source)</td>
</tr>
<tr>
<td>WMS</td>
<td>X</td>
</tr>
<tr>
<td>WFS</td>
<td>X</td>
</tr>
<tr>
<td>Desktop</td>
<td>X</td>
</tr>
<tr>
<td>Browser</td>
<td>X</td>
</tr>
<tr>
<td>Proxy</td>
<td>X</td>
</tr>
</tbody>
</table>
Technology Integration Experiment Webinar

- Afternoon of Thurs 18th November, 2010
- Approx 30 people turned up on the day
- EDINA, Snowflake, Cadcorp, Envitia, con terra, JRC, demonstrated:
  - Different clients (desktop, browser, proxy)
  - Different services (WMS and WFS)
  - Different federations (ESDIN and BKG)
OSI – Outcomes #1

- Using Shibboleth to protect OWS is practical
- Not particularly difficult on server side
- Not particularly difficult with browser based clients
- More subtle with desktop based clients but possible with some effort in short space of time; weeks, not months
- This kind of “IE testbed” approach appreciated by participating OGC members
- Operationalise and community support and tooling will be available
OSI/ESDIN Outcomes #2

Hard

From the European Interoperability Framework for Pan-European eGovernment Services (http://ec.europa.eu/idabc/servlets/Docb0db.pdf?id=31597)
INSPIRE Federation

Member State organisations, eg, NMCAs

Coordinating Centre

Key organisations, eg. EEA, JRC
Some options for going forward:

1. One Federation and every every legally mandated organisation joins
2. Multiple federations: one in each country and one pan-European.
3. One federation: one organisation in each country, the INSPIRE point of contact joins the single pan-European federation and acts as the gateway for all the other legally mandated organisations in the country that are standing up INSPIRE services.
4. Multiple federations: one in each country and inter-federation interoperability ensures SSO
All material will be available from:

http://igibs.blogs.edina.ac.uk/inspire2011/

Comments, questions, suggestions, etc, on blog very welcome

Or email: chris.higgins@ed.ac.uk
<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1600-1620</td>
<td>Introduction</td>
</tr>
<tr>
<td>1620-1640</td>
<td>Member States investigating use of Shibb for their NSDI’s</td>
</tr>
<tr>
<td>1640-1710</td>
<td>Demonstration of software working with the test Federation</td>
</tr>
<tr>
<td>1710-1730</td>
<td>Questions and concluding remarks</td>
</tr>
</tbody>
</table>