Shibboleth Access Management Federations as an Organisational Model for SDI

C.I. Higgins, M. Koutroumpas, A. Seales,
EDINA National Datacentre, Scotland
A. Matheus,
University of the Bundeswehr, Germany

INSPIRE Conference 2011,
Wednesday 29th June
ESDIN Project

- An eContentplus Best Practice Network project
- Resourced EDINA’s to investigate ESDI and Access Control
  - Principally using OGC Interoperability Experiments
- 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

Partners:
- National Technical University of Athens
- IGN Belgium
- EDINA, University Edinburgh
- 1Spatial
- EuroGeographics
- IGN France
- National Land Survey of Finland
- The Finnish Geodetic Institute
- Lantmäteriet
- Helsinki University of Technology
- National Agency for Cadastre and Real Estate Publicity Romania
- Kort & Matrikelstyrelsen
- Bundesamt für Eich- und Vermessungswesen
- Bundesamt für Kartographie und Geodäsie
- Universität Münster
- EuroGeographics
- Institute of Geodesy, Cartography and Remote Sensing
- National Agency for Catastrophe and Real Estate Publicity Romania
- University of Helsinki
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://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)
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”.
- Many accepted standards for securing these protected geospatial resources but no consensus which to use
  - 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
  - Scale back ambitions? or
  - Access Management Federations (AMF’s)? or, …?
What can Access Management Federations 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
• The members of the federation form a circle of trust and agree to a set of policies and technologies
• Provides **Single Sign On**
• My X-Border appl can now access a protected resource in country A, be challenged for credentials at home institution. Now I can also access additional federation resources (if authorised) in country A, B, C, …, **without** needing to re-authenticate
One Solution - 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
• Paper submitted to the International Journal SDI Research to accompany this presentation
• Premise is that a concomitant security infrastructure is necessary to realise SDI objectives where protected resources are involved
• Table 1 posits:

“Twelve required attributes for a solution to securing SDI”
1. Based on open security interoperability standards
   - Security Assertion Markup Language (SAML) from OASIS
2. Works across administrative domains
   – Fundamental reason for Access Management Federations
3. Single Sign On

- Basic Use Case for SAML
- Principals authenticate at one web site, access the resource of interest, and are then able to access additional protected resources at other web sites without having to re-authenticate
4. Does not require any changes to the OGC interfaces being protected

- OGC Interoperability Experiments have demonstrated use with range of familiar industry implementations, eg, geoserver, mapserver, Snowflake
- No need for SOAP bindings
5. Requires minimal changes to the OGC Web Service clients

- SAML 2 ECP must be implemented
- Reference implementation available
- 6 organisations through OGC Interoperability Experiment have made changes
- Some products now commercially available
- Browser relatively easy, desktop harder
- Took weeks, not months
6. Proven production strength
   – Already in daily use by millions
   – Possibly already in your country
7. Satisfies data privacy requirements
   - What set of SAML assertions are required for pan-European SDI authorisation decisions?
8. Flexible in order to accommodate a wide variety of different use cases

- Different SAML workflows
  - Portal flow
  - Service Provider flow

- SAML already used by GI community
  - European Space Agency “User Management Interfaces for Earth Observation Services”
  - Where are the interoperability points?
9. Should be an open source “reference implementation”
   – Shibboleth
10. Not geospatial specific and in widespread mainstream IT use
   – Leverage broad participation in technology development
   – Stay flexible as much as possible
   – Maximise potential for interoperability
11. Should, in so far as is possible, be built on information systems already in place

- Huge amount of prior investment in identity management
- Organisations know best how to manage their users
- Many Shibb Federations in place already in academic sector across Europe
  - A source of expertise, collaboration and potentially extremely valuable interoperability link across sectors
12. Should not be centralised
   - No huge databases with users credentials
   - Needs to be decentralised to scale
Hard

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

1. One Federation and 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