International Journal of Spatial Data Infrastructures Research, 2012, Vol.7, 107-124.

Shibboleth Access Management Federations as an Organisational Model for SDI·

Christopher I. Higgins[1], Michael Koutroumpas[1], Andreas Matheus[2], Andrew Seales[1]

[1]EDINA, University of Edinburgh
chris.higgins@ed.ac.uk; m.koutroumpas@ed.ac.uk; andrew.seales@ed.ac.uk

[2]University of the Bundeswehr, andreas.matheus@unibw.de

Abstract

Shibboleth is an open source implementation of the OASIS standard Security Assertion Markup Language (SAML). Shibboleth Access Management Federations (AMFs) are used daily around the globe by millions of users – mainly in the academic realm – in order to securely exchange the identity information necessary to make authorisation decisions concerning protected web resources. AMFs are typically comprised of a number of entities, eg, organisations working together to achieve a set of shared objectives while each member retains control over its own internal affairs. There are three main categories of entities: identity management is devolved to individual member organisations who act as *Identity Providers*, *Service Providers* are established by organisations wanting to make protected resources available, and finally, there is a small *Coordinating Centre*. Principally through the European Spatial Data Infrastructure Network (ESDIN) project and the OGC Web Service (OWS) Shibboleth Interoperability Experiment, it has been established that Shibboleth provides a production strength, standards based, open source, interoperable mainstream IT solution to the problem of how to implement AMFs around the OWS central to SDI's. Furthermore, it has been demonstrated using a prototype federation of INSPIRE compliant services established under ESDIN that this can be done without modifications to either mainstream Shibboleth or OWS. However, non browser based clients require adaptation. Various options exist as to how the main actors within a European

DOI: 10.2902/1725-0463.2012.07.art6

SDI/Federation may organise themselves in order to realise the objective of allowing authorised users from key organisations, eg, EU bodies concerned with environmental policy formation, seamless access to harmonised protected geospatial information through OWS. This paper proposes that a parallel security infrastructure is necessary to realise SDI where protected resources are involved and gives an account of work undertaken demonstrating how Shibboleth based AMF's meet this need.

Keywords: security, access control, authentication, Shibboleth, SAML, Open Geospatial Consortium, interoperability experiments, web services, access management federations, WMS, WFS

1. INTRODUCTION

Security is an important topic in the development of Spatial Data Infrastructures (SDI) that is often neglected or misunderstood and which often ends up presenting an insurmountable barrier preventing SDI initiatives from meeting their initial ambition. For a wide variety of different reasons; commercial, national security, data protection/privacy, etc, much valuable data is protected, and while the "open agenda" has enjoyed huge success and grown significantly over the past few years, the reality is that a significant amount of the most valuable data is going to stay protected.

If this statement is acknowledged as true and we want SDI to reach their full potential and make accessible the widest possible range (open and protected) of data, services and other resources, then a genuinely interoperable solution to the problem of how to share protected resources across administrative domains needs to be found.

As with INSPIRE and its provision that it *"…shall build upon infrastructures for spatial information established and operated by the Member States."*, (European Parliament and Council, 2007), it should be a guiding principal that any potential solution – besides addressing all relevant security concerns - should have minimal impact on existing operational systems.

2. SCOPE AND LICENCING

This paper does not cover to any significant extent the related issues of geospatial rights management, e-commerce, licencing, licence negotiation,

licence enforcement or authorisation. We are concerned primarily here with the fundamental issues of access control and authentication.

Our starting point is: wherever it is necessary to control access to online resources for whatever reason, it is a fundamental pre-requisite that you be able to identify who (or what) is trying to access your protected resource. Everything else is predicated on this ability.

To make the problem tractable and provide meaningful demonstrations we limit the discussion to situations where "framework agreements" are in operation. In the language of INSPIRE, "*framework agreement",* may be defined as *"an arrangement that includes two or more partners and covers the conditions for access and use of one or more data sets and services established prior to use*"[1]

Framework agreements are widespread. Examples in the UK public sector include the One Scotland Mapping Agreement[2] and the recently launched (April 2011) Public Sector Mapping Agreement for England and Wales[3]. Within the UK academic sector, the Ordnance Survey (the UK's National Mapping Agency) EDINA Digimap licencing arrangement is a typical framework agreement in respect of how many of the most significant geospatial datasets are made available to the academic sector.

The relationships involved in establishing and operating Framework Agreements can be complicated. In the context of this paper though, the key points are that end users need know nothing about this complexity - the service is free at the point of use. However, the end users do need to identify themselves so that technically the relationships can be verified.

For the purposes of this report, the real world use cases most obviously catered for are where framework agreements are in operation; where licences are negotiated "out of band", access restrictions are indicated in service and dataset metadata, and content is free at the point of use for authenticated and authorised users.

Note though, that in maintaining this "separation of concerns", that the other aspects of security mentioned above (geospatial rights management, e-

[1] http://inspire-forum.jrc.ec.europa.eu/pg/pages/view/26345/framework-agreements [accessed May 2011]
[2] http://www.ordnancesurvey.co.uk/oswebsite/public-sector/scotland/index.html [accessed May 2011]
[3] http://www.ordnancesurvey.co.uk/oswebsite/public-sector/mapping-agreement/index.html [accessed May 2011]

commerce, licencing, licence negotiation, licence enforcement, authorisation) may be added on in a modular fashion to the fundamental work described here.

It is a premise of this paper that if broad agreement can be reached on a standards based interoperable solution to access control then it will facilitate making progress with addressing other important outstanding interoperability questions relating to sharing of data in SDI.

3. AUTHENTICATION

Authentication is a mandatory part of access control and is concerned with establishing that claims made concerning a subject who is attempting to use a particular resource are authentic, ie, true. Typically, this involves confirming a subjects identity. This kind of information is essential before it can be determined that the subject is authorised to access the resource.

SDI is underpinned by open geospatial interoperability standards from primarily the Open Geospatial Consortium (OGC) and ISO TC/211. The key OGC interfaces (we concentrated on Web Map Service (WMS) and Web Feature Service (WFS)) are agnostic about how they may be secured and it is left to the discretion of implementers and individual circumstances. The result is that there is a proliferation of point solutions with no widely accepted dejure or defacto standards. Consequently, there is little genuine cross administrative domain interoperability in SDIs where protected resoures are concerned.

As the directive allows public access to be limited, INSPIRE is very much a case in point. Across the European member states, we currently have the situation where public authorities are publishing services but controlling access to many (often the most valuable data) using a range of different, incompatible, unrelated techniques.

We would contend that, in order to claim to be a genuinely interoperable solution to the problem of cross adminstrative access control around OGC Web Services, any widely adopted solution should have the characteristics identified in table 1.

The rest of this paper is primarily concerned with investigating whether Access Management Federations based on Security Assertion Markup Language (SAML) meet these requirements. Specifically, we examine whether Shibboleth[4] (an open source implementation of SAML) meets the needs of the those elements of the geospatial community who agree that a complementary security

[4] http://shibboleth.internet2.edu/ [accessed Jan 2012]

infrastructure is necessary to enable SDI involving protected resources to meet their full potential.

Table 1: Twelve Desirable Attributes for a Solution to Securing SDI

1	based on open security interoperability standards
2	works across administrative domains
3	Single Sign On (SSO) implementation, ie, principles 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
5	requires minimal changes to OGC web service clients
6	proven production strength
7	satisfies data privacy requirements
8	flexible in order to accommodate a wide variety of different use cases
9	should be an open source “reference implementation”
10	not geospatial specific and in widespread mainstream IT use
11	should, in so far as is possible, be built on information systems already in place
12	should not be centralised

4. SECURITY ASSERTION MARKUP LANGUAGE (SAML)

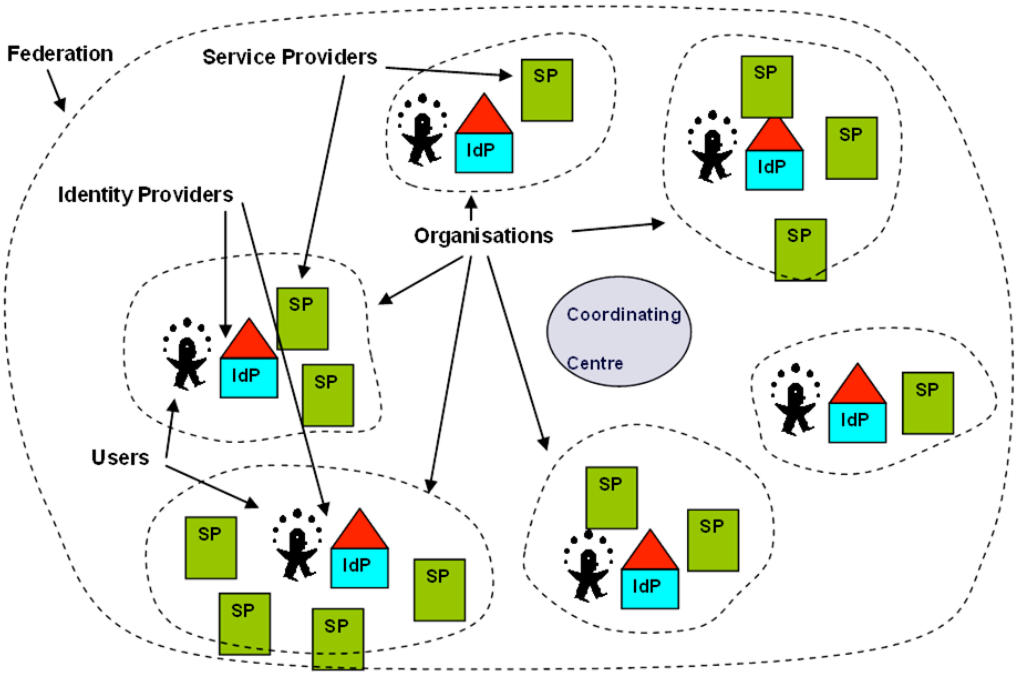
SAML is an open standard of the OASIS Security Services Technical Committee, whose primary purpose is to enable authentication data across security and policy domains by defining the means for a secure exchange of Extensible Markup Language (XML) encoded assertions.

The main use case for SAML is Single Sign On (SSO): where users authenticate at one web site, access the resource of interest if they are authorised, and are then able to access additional protected resources at other web sites participating in the same SSO network without having to authenticate again. SAML enables the secure communication of authentication information from the first site to additional sites in different security/administrative domains, these sites can then decide whether the user is authorised to access the protected resource or not.

An organisational pre-requisite for this kind of SAML scenario is the existence of an access management federation (alternatively called identity management federations). In this instance, federation is taken to mean a group of organisations with common business goals which has established a circle of trust and formal understanding with associated procedures so that these cross-domain business interactions can take place. Note that depending upon factors such as scale, eg, national or international, number of organisations, degree of similarity, etc, establishing these arrangements can be a non-trivial undertaking.

Most organisations with valuable online resources have some form of identity management in place, the decoupling and abstraction of identity management in federations required to make these cross security domain decisions is standardised in SAML. In Figure 1; the Service Provider (SP) role is assumed by organisations that want to make protected resources available and the role of Identity Provider (IdP) is assigned to organisations which want to manage their own user credentials and have their users participate to be able to access the protected resources provided by the SPs.

Figure 1: Key Roles within a Typical SAML Access Management Federation[5]



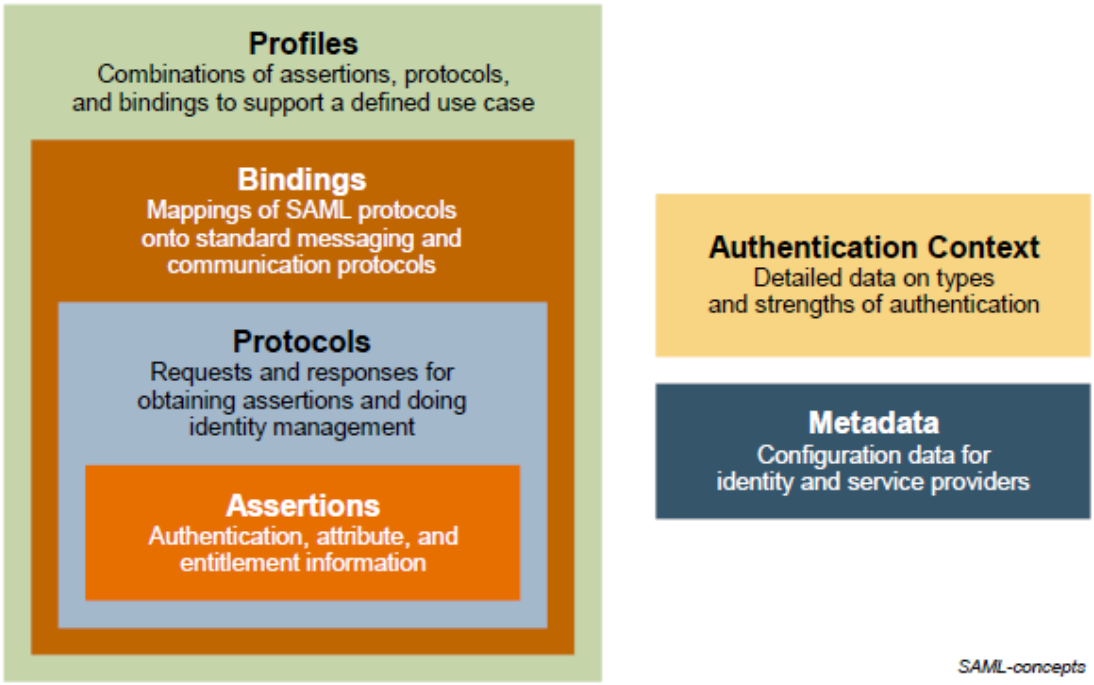
A key aspect is formal agreement on what security and identity information concerning the agent who is accessing the protected resource is required to enable decisions to be taken as to whether they are authorised to access the resource or not - this information is communicated as assertions.

Figure 2 provides some fundamental information on the basic concepts of SAML and serves to illustrate some of the flexibility of SAML as these basic concepts can be combined in various ways to meet the requirements of multiple use cases.

[5] Adapted from a diagram on the Switch (Serving Swiss Universities) website: http://www.switch.ch/aai/about/federation/ [accessed May 2011]

- **Assertions** are basic packets of information containing statements about a principal (which wants to access the protected resource) that an asserting party, ie, an IdP, claims to be true. The SP then uses this information to make access control decisions. This attribute based model gives great flexibility, eg, under circumstances where the principals full identity is not important, cannot be shared for data privacy reasons, or is insufficient for an authorisation decision without additional information.
- **Protocols** describe how packaged assertions are exchanged with SAML request and response elements, and gives the processing rules that SAML entities must follow when producing or consuming these elements.
- **Bindings** are mappings of SAML protocol message onto standard messaging formats and/or communications protocols, eg, Hypertext Transfer Protocol Secure (HTTPS).
- **Profiles** describe in detail how SAML assertions, protocols, and bindings are used together to support a defined use case. In the context of this paper, two profiles are of immediate interest: the Web Browser SSO Profile and Enhanced Client or Proxy (ECP) Profile.

Figure 2: Basic SAML Concepts



Source: OASIS, 2008

5. SHIBBOLETH

Shibboleth is an initiative from the US based Internet2 research and education networking consortium used primarily in the academic sector. It is an open source package that allows the establishment of federations and may be considered as a "reference implementation" for SAML. It is a production strength solution to the problem of how to securely exchange user information based on open standards. Shibboleth is being used daily by millions of users, eg, 8 million in the UK federation alone, around the globe and there are Shibboleth based access management federations in most developed countries, including most of Europe.

Table 2: Examples of Worldwide Shibboleth Federations[6]

Europa	Amerika	Australien
CRU (Frankreich)	InCommon (USA)	MAMS
DFN-AAI (Deutschland)	InQueue (USA Testföderation)	
DEMOaar (Deutschland Testföderation)		
DK-AAI (Dänemark)		
ENTREE (Niederlande)		
SURFNET (Niederlande)		
FEIDI (Norwegen)		
LUDIT-AAI (Belgien)		
HAKA-Federation (Finnland)		
SWAMID (Schweden)		
SWTICH-AAI (Schweiz)		
UK Access Management Federation for Education and Research (Vereinigtes Königreich Großbritannien und Nordirland)		

As indicated in the text above, in the belief that enterprises themselves are best positioned to manage the identities of their members, the philosophy behind Shibboleth/SAML is to devolve responsibility as much as possible. Note the arrangement represented in Figure 1 is simplified and that other configurations are possible, eg, one large institution may setup an IdP and run it on behalf of several smaller institutions as well as itself.

There are still some components that must be centralised and under the control of the Coordinating Centre. Using the example of the UK Access Management Federation, these functions include:

[6] Deutsches Forschungsnetz (DFN): https://www.aai.dfn.de/links/ [accessed May 2011]

- running the main WAYF (Where Are You From) or DS (Discovery Service), effectively a list mapping institution names to IdP Uniform Resource Locators (URLs).
- maintaining and publishing the federation metadata describing participating entities. This provides the information required for entities to know how to communicate with each other, and establishes a trust fabric permitting entities to verify each other's identities
- user support, eg, for software upgrades
- enacting and informing federation policy, eg, for attribute release from the IdP's, attribute request from the SP's
- procedures for joining and leaving the federation

Note that PKI trust fabric is used by many Shibboleth federations including the UK AMF. A full treatment of the different models which can be used is beyond the scope of this paper. The reader is referred to (Young, 2010) for a statement of the current position in the UK.

6. SHIBBOLETH RELATED OGC INTEROPERABILITY EXPERIMENTS

OGC Interoperability Experiments (IE) are intended as relatively simple, low overhead, means for OGC members to get together and, facilitated by OGC staff, advance specific technical objectives within the OGC baseline. They are more lightweight than the OGC Web Services initiatives and are intended to be focussed on specific interoperability issues. All effort is viewed as voluntary and supported by in-kind contributions by participating member organisations. The duration is normally of the order of 6 months or so as identified in the IEs activity plan. There have been two Shibboleth related IE's in the last two years.

6.1. Authentication IE

Partly as a consequence of work undertaken in the JISC[7] funded Secure Access to Geospatial Services (SEE-GEO) project demonstrating how Web Map Services (WMS) can be protected using Shibboleth, and partly in recognition that an approach to authentication acceptable to the open geospatial standards community is both important and missing, the OGC Security Working Group initiated discussion on an Authentication Interoperability Experiment. The formal kickoff was held in association with the Mountain View Technical Committee (TC) meeting in Sept 2009.

The aim of the Authentication Interoperability Experiment was to test standard ways of transferring authentication information between OGC clients and OGC services by leveraging mechanisms already existing in the transport protocol

[7] http://www.jisc.ac.uk/ [accessed Jan 2012]

(HTTP and SOAP). The original idea was to test the following mechanisms: HTTP Authentication, HTTP Cookies, SSL/X509, SAML, Shibboleth, OpenID and WS-Security.

The main output from this activity was an Engineering Report (OGC, 2011) approved by the OGC in Dec 2010.

At the time this IE was initiated, the EU-funded, Eurogeographics led, European Spatial Data Infrastructure Network (ESDIN[8]) project was underway. With the agreement and support of the ESDIN consortium (Higgins, 2011), EDINA participated in this IE and concentrated on testing SAML2 based SSO authentication for a small federation (the ESDIN Federation) of protected OGC Web Services (OWS).

The main outcomes from the ESDIN participation in this experiment were:

- Further evidence that it is possible to protect WMS using Shibboleth
- No changes to the standard OGC interface. Their is no need to use SOAP (though note there is no reason why Shibboleth would not work with SOAP were it required)
- No changes to the standard Shibboleth download
- Changes **are** required to the OWS desktop clients.

In the course of this IE, EDINA developed and demonstrated two clients: one desktop (based on OpenJump[9]) implementing the SAML Enhanced Client or Proxy (ECP) Profile (OASIS, 2005) and one browser based (OpenLayers[10]) implementing the SAML Web Browser SSO Profile.

6.2. OWS Shibboleth IE

Throughout the ESDIN project, as part of broader awareness and dissemination activities, it was policy to engage with a wide variety of stakeholders to encourage discussion and ideas from a wide variety of organisations and individuals as to how to take the project forward. In one such discussion, it was suggested by a representative from a GIS vendor that a good way of encouraging the software producing members of the OGC to modify their client software to be able to undergo the Shibboleth/SAML interactions was to hold an event where a variety of software producers publicly demonstrated their software working with the ESDIN federation.

[8] http://www.esdin.eu/ [accessed May 2011]
[9] http://www.openjump.org/ [accessed Jan 2012]
[10] http://openlayers.org/ [accessed Jan 2012]

After discussion with the OGC it was decide to cast this “plugfest” or “Technology Integration” type event as an IE. A press release inviting participation in the OGC Web Service Shibboleth Interoperability Experiment (OSI) was issued on the 31st Aug 2010 with the first meeting taking place during the Toulouse TC in September 2010.

The stated aim in OSI was to provide the OGC software producing community with the means and opportunity of modifying their OWS client software to be able to work with Shibboleth Access Management Federations. The emphasis was on desktop clients as this is harder than browser based clients and having a range of different proprietary and open source client types demonstrated is more valuable. We would then provide the participants with the opportunity to demonstrate their software in action by granting temporary access to the ESDIN federation and Secure Dimensions GmbH.

To achieve the above; EDINA managed the IE, provided an open source reference implementation of a modified desktop client (the Open Jump client), provided technical support and organised the Technology Integration Experiment event as a webinar.

The webinar took place on the afternoon of Thurs 18th Nov, 2010. Approximately 30 people attended and the following organisations all demonstrated modified OWS clients accessing ESDIN federation protected services: EDINA, Snowflake, Cadcorp, Envitia, con terra and the EU’s Joint Research Centre.

At the end of the webinar, we had demonstrated different clients (desktop, browser, proxy), different services (WMS and Web Feature Service (WFS)), and different federations: ESDIN and a test federation established by the BKG (the German National Mapping Agency). A draft OGC Engineering Report has been produced with the final report due for publication in 2012.

7. SHIBBOLETH FOR SECURING SDI

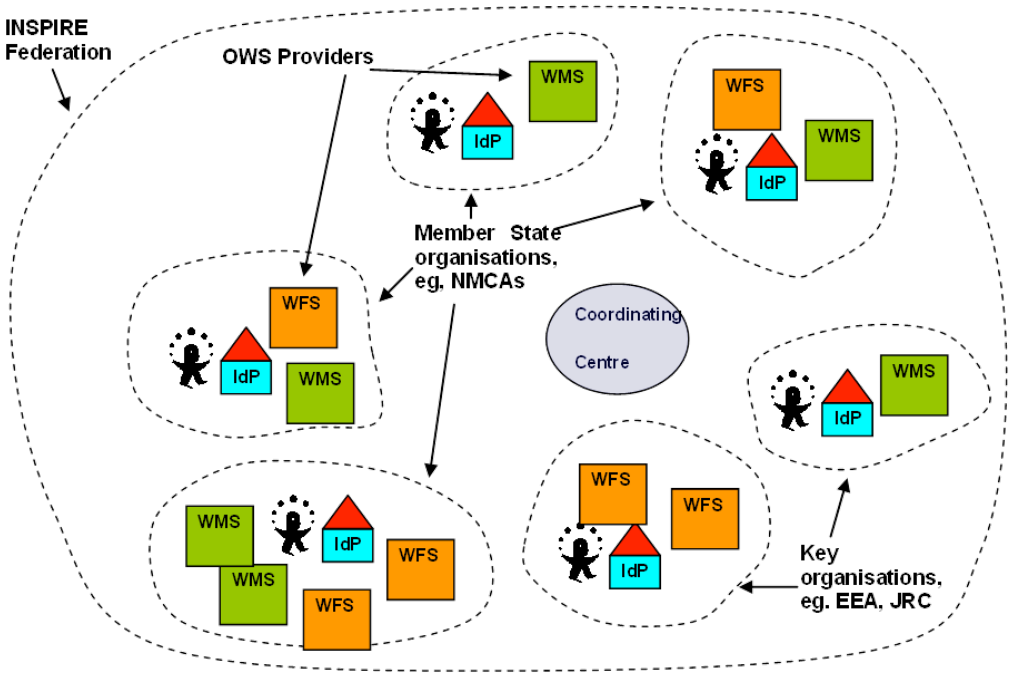
Probably the most significant outcome from the above activity is that we have demonstrated that technically, Shibboleth can be used to provide a production strength solution to securing SDI. By production strength, we mean a standards based solution that demonstrably works using technology that is currently in operation and being used by large numbers of organisations and people in many different countries (see table 2).

On the server side, it is technically straightforward to install and configure Shibboleth to protect unprotected, unmodified OWS established using any OGC standards compliant software. On the client side, modifications are necessary but doable. Experience with a range of different clients shows that browser based

clients are easy and desktop based clients harder. The software producing participants in the OWS Shibboleth IE modified their clients in weeks, not months, and several are making their offerings commercially available. If the decision is taken to operationalise this approach, then it is reasonable to expect that support and tooling from the GI community will be forthcoming.

Figure 3 builds on Figure 1, it illustrates how in the kind of pan-European scenarios that ESDIN was concerned with that the Service Providers are INSPIRE points of contact (often National Mapping and Cadastral Agencies (NMCAs)) and that the services being provided can be either WMS or WFS services.

Figure 3: A Possible Evolution for the ESDIN Federation



Source: Higgins, 2011

There are a number of different ways the different roles within the federation can be filled. For example, each organisation can become an Identity Provider (IdP) itself, or a larger organisation can fulfill this role on behalf of several smaller organisations.

In an INSPIRE context, it is likely that there will be more than one public authority within each member state standing up protected services. This leads to several (non-exclusive) options:

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.

Option 1: Unlikely as not every public authority in every country is going to have the capacity. Even within the ESDIN project, with resourcing and expert technical support to hand, it proved difficult to persuade NMCAs to join.

Option 2: Possible in some cases, eg, where the members states own national e-government interoperability framework mandates the use of SAML for transferring identity information. On the other hand, it is difficult to see this happening where member states already have major commitment and investment in alternative means of identity management, eg, the UK's Government Gateway .

Option 3: May be the most practical intermediate step.

7.1. Shibboleth and the Academic Sector

Shibboleth is used primarily in the academic sector and one consequence of its wider uptake by the geospatial community which should not be underestimated would be the potential for improved interoperability bertween the public and academic sectors.

Evidence (Medyckyj-Scott et al, 2011) suggests that the academic sector often gets neglected when SDI's are being planned and developed. A consequence of this is that graduates are often ill equipped with the skills necessary to enable full exploitation of interoperable SDI technology, neither are they familiar with using reference data from public authorities, and the public sector finds that its research and development requirements are not adequately addressed

There is an active open source community around Shibboleth and a pool of expertise in its use and administration within the academic sector. It is in the geospatial communities interest to leverage this capacity and maintain links with existing national federations. The technology we use for securing SDI should be mainstream and care should be taken that we do not go down a geospatial specific path so that we can leverage broader developments. In the case of Shibboleth/SAML, a good current example would be inter-federation

interoperability - an active area of research and development within the internet security community.

8. RELATED WORK – OPENID

Shibboleth/SAML is not the only technical option for access management federations and OpenID is emerging in the geospatial community as a serious alternative with current examples to be found within the Earth Systems Grid, eg, Siebenlist et al, 2009, and the Global Earth Observation System of Systems (GEOSS) communities, eg, GEOSS, 2011

In this respect, it may be worth considering some of the findings from the JISC funded Review of OpenID (Chadwick, 2008), see Table 3 below.

Table 3. Comparison of Features of OpenID and Shibboleth as implemented in the UK Federation (adapted from Chadwick, 2008)

Feature	OpenID	Shibboleth/UK Federation
Ease of understanding/ simplicity of specifications	Simple	Complex
Implementation effort	Relatively Low	Relatively High
WAYF service	Not needed	Needed
User Registration	Zero assurance of who the user is	Almost always linked to a real person
Trust Infrastructure	None specified	IdPs can state they can always identify the real life person
Re-allocation of IDs	Yes, can be done	Yes, can be done, but not designed to be life-long
Privacy Protection	None. IdP and SP can track users between sessions (except that users can be anyone and can change their OpenIDs frequently).	SP cannot track user between sessions, but IdP can track which SPs user is interacting with
Phishing	Very susceptible	Very susceptible unless users scrutinize X.509 certificates carefully.
Cross Site Request Forgery	Very susceptible	Not susceptible
Dependency on IdP for 24x24 service	Yes	Yes
Few high-value SPs	Yes	No

In the authors opinion, it is not proven that OpenID meets the attributes itemised in table 1 and it is unlikely that the technology is sufficiently secure to persuade a

majority of content providers to expose their most valuable holdings available over the internet to users authenticated this way.

9. DISCUSSION AND CONCLUSIONS

As SDI implementations progress it is the authors opinion that it will increasingly become clear that a concomitant security infrastructure that operates across administrative domains is necessary in order to make SDI viable where protected resources are involved.

The current debate in respect of OpenID and Shibboleth/SAML is a good example of what makes security difficult. It is a complex issue and it is difficult to understand important issues without being deeply involved with the internet security community. One of the main differences relates to privacy (with openID there is no assurance of who the user is) with all the attendant policy issues associated with managing online user identity information.

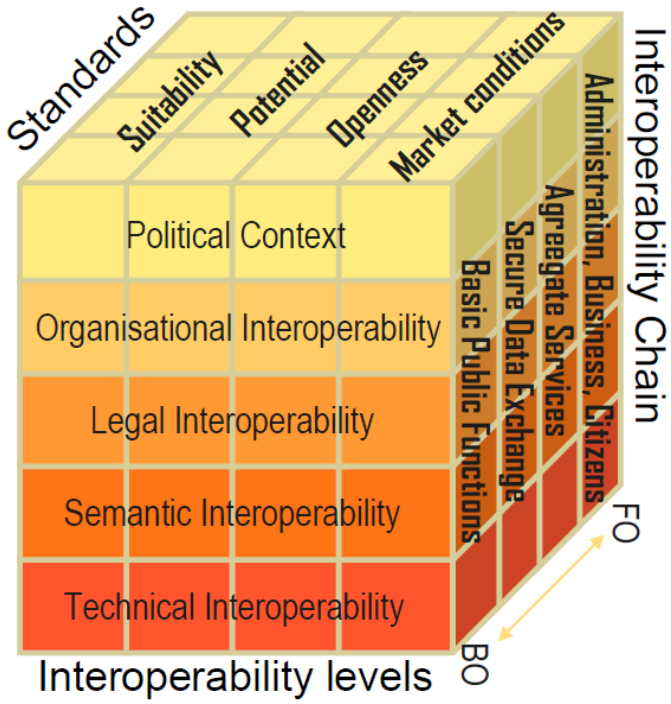
As Figure 4 illustrates, the situation becomes an order of magnitude harder when the considerable legal, political and organisational aspects are taken into consideration, not to mention the financial implications.

To progress this work, possibly the best course is to begin by clearly acknowledging that, unless SDI ambitions are scaled back, or its made a pre-requisite that all resources are open, then a complementary cross-administrative domain security infrastructure is required with associated research and development programme.

Table 1 provides a starting point based on what we think the characteristics of such a security infrastructure should be. It is our opinion, that there is a need for a thorough engagement with the main SDI content providers to discover what it would take to persuade them to make their most valuable resources, eg, protected data and services, available online across administrative domains. One view onto the results from such a study could be a set of transverse use cases that could be mapped to SDI governance procedures.

The Shibboleth/SAML solution presented above demonstrably works, it meets the requirements articulated in table 1, engages the academic sector, and is designed from the ground up to integrate with existing identity management systems. However, as indicated in Figure 4, technical interoperability may very well turn out to have been the easy bit.

Figure 4: Dimensions of Interoperability



Source: IDABC, 2008

We conclude this paper with a summary of what we consider some of the priorities for future related work.

9.1. Future Work

- **Service Chaining:** In terms of architecture patterns for service chaining (ISO, 2003), the solution presented above only works for "transparent" chaining, ie, where the user knows the details of the services being invoked. Where protected services are involved in association with the more advanced chaining patterns, ie, "translucent" and "opaque" chaining; where the user invokes a service that in turns invokes a number of other services, it could be necessary to have a means of authenticating users for services other than the one initially invoked.

- **Inter-federation interoperability:** It is already the case that individuals may belong to more than one federation and it is likely that as federated approaches expand this will become more common. Numerous scenarios may also be envisaged where for some purposes a user, eg, working with a

cross-border pan-European application, needs to access national data. In accordance with the organisational model outlined in Figure 3, this resolves to a problem of interoperability between a pan-European federation and national, sub-national or thematic federations.

- **Interoperability with OpenID:** As identified in Chadwick, 2008, and elsewhere within the Shibboleth and OpenID communities, there is no technical reason why both protocols cannot be used within the same or different federations. It is up to the service providers to decide who or what they trust.

- **Interoperability with other uses of SAML:** The perceived complexity of SAML is one of its strengths as well as one of its weaknesses. It allows for great flexibility enabling a wide variety of use cases. For example, various profiles may be supported and individual SAML components may be used in isolation. A consequence of this is that SAML is already widely used both in mainstream IT and within the geospatial community, eg, OGC, 2010.

REFERENCES

Chadwick, D. and S. Shaw (2008). Review of OpenID, at http://www.jisc.ac.uk/media/documents/programmes/einfrastructure/openid-finalreport-v1.0.pdf [accessed 29 May 2011].

European Commission (2007). *Directive 2007/2/EC of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)*. Official Journal of the European Union, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007L0002:EN:NOT [accessed 28 May 2011].

GEOSS (2011). Engineering Report GEOSS Architecture Implementation Pilot, Phase 3, Version 1.0 at http://www.ogcnetwork.net/pub/ogcnetwork/GEOSS/AIP3/documents/GEOSS_AIP3_Summary.pdf, [accessed 19 January 2012].

Higgins, C. (2011). "Operational view/download services and access control conforming to INSPIRE implementation rules into the academic sector geospatial testbed(s)", *ECP-2007-GEO-317008, ESDIN* at http://www.esdin.eu/sites/esdin.eu/files/ESDIN%20D11%206%20services%20academic%20sector%20v4%200.pdf [accessed 29 May 2011].

IDABC (2008). European Interoperability Framework for Pan-European eGovernment Services, Draft document as basis for EIF 2.0 at http://ec.europa.eu/idabc/servlets/Docb0db.pdf?id=31597 [accessed 31 May 2011].

ISO/TC 211 (2003). IS 19119 Geographic Information – Services. N 1540. *ISO/TC 211 Geographic Information/Geomatics.*

Medyckyj-Scott, D., Sutton, E., Higgins, C. and I. Heywood (2011). The European National Mapping and Cadastral Agencies and Higher Education, *A Market for Geospatial Information – Myth or Reality*, at http://plone.itc.nl/agile/initiatives/Spatial%20Data%20Access%20Final%20Report.pdf [accessed 29 May 2011].

OASIS (2005). Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, *OASIS Standard*, 15 March 2005, at http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf [accessed May 29 2011].

OASIS (2008). Security Assertion Markup Language (SAML) v2.0 Technical Overview, Committee Draft 02, 25 March 2008, at http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf [accessed 22 May 2011].

Open Geospatial Consortium (2010). User Management Interfaces for Earth Observation Services, 07-118r8 at http://portal.opengeospatial.org/files/?artifact_id=40677 [accessed 10 February 2012].

Open Geospatial Consortium (2011). Authentication for OGC Web Services, 10-192 at http://portal.opengeospatial.org/files/?artifact_id=41734 [accessed 28 May 2011]

Siebenlist, F., Ananthakrishnan, R., Bernholdt, D.E., Cinquini, L., Foster, I.T., Middleton, D.E., Miller, N. and D.N. Williams (2009) "Enhancing the Earth System Grid Security Infrastructure through Single Sign-On and Autoprovisioning", *Proceedings of the 5th Grid Computing Environments Workshop, SC09.* at http://www.mcs.anl.gov/uploads/cels/papers/P1683.pdf [accessed 29 May 2011].

Young, I. A. (2010). Federation Technical Specifications, *UK Access Management Federation for Education and Research*. 9 September 2010, at http://www.ukfederation.org.uk/library/uploads/Documents/federation-technical-specifications.pdf [accessed 28 May 2011].