

# **Final Report for the JISC funded Dynamic Virtual Organisations in e-Science Education (DyVOSE) Project**

Date  
28<sup>th</sup> February 2007

## Authors

Prof Richard O. Sinnott <sup>1</sup>	National e-Science Centre	University of Glasgow
Prof David W. Chadwick	Information Systems Security Group	University of Kent
Dr Sassa Otenko	Information Systems Security Group	University of Kent
Dr John Watt	National e-Science Centre	University of Glasgow
Dr Jos Koetsier	National e-Science Centre	University of Edinburgh
Dr Dave Berry	National e-Science Centre	University of Edinburgh
Tuan A. Nguyen	Information Systems Security Group	University of Kent

## Document History

Prof Richard O. Sinnott	Draft version 1.0	23 February 2007
Prof David W. Chadwick	v.1.1	25 February 2007
Dr John Watt	v.1.2	26 February 2007
Prof Richard O. Sinnott	v.2.0	26 February 2007

---

<sup>1</sup> Contact person.

## Table of Contents

Acknowledgements .....	4
Executive Summary .....	5
Background .....	7
1. Aims and Objectives.....	8
2. Methodology.....	9
3. Implementation.....	11
4. Outputs and Results.....	12
5. Outcomes.....	14
6. Conclusions.....	14
7. Implications .....	15
8. References .....	16
Appendixes .....	17

## **Acknowledgements**

*This project was funded as part of the Joint Information Systems Committee (JISC) Core Middleware Technical Development programme. The project partners at Glasgow, Edinburgh and Kent (formerly Salford) would like to thank JISC and the programme managers (James Farnhill, Nicole Harris and Ann Borda) for providing excellent support throughout the course of the project. Thanks are given especially for the various extensions to the life time of the project to support the dissemination of project results.*

*Thanks are also given to Dr Sandy Shaw and the SDSS support team for answering questions on issues related to Shibboleth and in providing the federation used as part of the DyVOSE explorations.*

*Dr Mark Norman and Alun Edwards at the University of Oxford are acknowledged for the joint work undertaken in ESP-Grid.*

*Dr Ian Piper from Glasgow Southern General Hospital is acknowledged for the data sets and scenarios explored within the neurological domain.*

*For the various case studies used to demonstrate DyVOSE results, acknowledgements are given to the Department of Trade and Industry for the Biomedical Research Informatics Delivered by Grid Enabled Services (BRIDGES) project; to JISC for the Exploring Shibboleth and Public Key Infrastructures (ESP-Grid) project; to JISC for the Glasgow early adoption of Shibboleth (GLASS) project; to the Medical Research Council (MRC) for the Virtual Organisations for Clinical Trials and Epidemiological Studies (VOTES) project; and to the Biotechnology and Biological Sciences Research Council (BBSRC) for the Grid Enabled Microarray Expression Profile Search (GEMEPS) project.*

## Executive Summary

The overall aim of the DyVOSE project was to explore how dynamic Grid based virtual organisations (VOs) could be established building upon advanced authorisation infrastructures – specifically through extensions to the Privilege and Role Management Infrastructure Standards Validation (PERMIS) technology ([www.openpermis.org](http://www.openpermis.org)). The application area of DyVOSE was the education domain however the results of the project are far reaching and can (and are) being used to support e-Research related activities more generally.

Fundamentally, DyVOSE recognised that future Grids require more advanced security infrastructures that go beyond existing authentication-only based approaches (*I know who you are and here is a local account for you to use, e.g. to compile and run arbitrary codes*), to authorisation-driven approaches (*I know who you are and this is what you are allowed to do on my resource and I will define/check/enforce this*). To support this model in a manner that catered for the dynamicity and scalability concerns of current and future Grids required novel enhancements to existing state of the art authorisation techniques, both in how authorisation infrastructures are established dynamically and how they are subsequently used to enforce authorisation policies across multi-institutional Grid based resources. In establishing and managing large-scale Grids, a single administrator is unlikely to be solely responsible for resources across their own institution, e.g. there is no single administrator for the University of Glasgow, and almost certainly will not be responsible for resources across remote collaborating institutions. In this context, the approach taken within DyVOSE was based upon delegation of authority: allowing an administrator to delegate a level of privilege to (trusted!) local or potentially remote individuals. This privilege allowed influencing local security infrastructures in a scalable, but tightly controlled manner. This was realised through a Delegation Issuing Service (DIS) which allowed privileged users, e.g. local system administrators or resource managers, to allocate restricted sets of roles to those trusted individuals at potentially remote sites, who depending on the delegation policy, could potentially further delegate these roles to other users at other sites. Presentation of these delegated roles (given as digitally signed security attributes) to the resource provider could then be used to enforce the resource or VO-specific authorisation policy.

This model has several direct benefits to future Grids (and Grid based research). Firstly, a fundamental tenet of the Grid is that sites should be autonomous, i.e. define and enforce their own security policies on access and usage of local resources. This model allows local sites to define who can access their resources and under what circumstances in a manner that does not require them to explicitly grant access to known lists of collaborating individuals, or allow other people to set the access control policy for their site. Rather, building on the role based access control model of PERMIS, sites can delegate the authority to remote trusted individuals to allocate roles to their local users, and potentially depending on the delegation issuing policy, further delegate the authority to issue these roles to other parties at other remote institutions. Thus the model is scalable but also very secure whilst retaining tight control over what users can do, since the local administrator always has control over which privileges these roles are allowed to have. Since the roles are assigned in digitally signed attribute certificates, it is not technically possible for an unauthorised user to forge one of these certificates and thus gain unauthorised access.

Secondly this model supports usability aspects of Grid infrastructures. One of the key issues to be addressed in encouraging the uptake of Grids and e-Research more generally is the complexity of existing PKI based approaches. Having to obtain X509 digital certificates and convert them to formats suitable for Grid technologies is a fraught process for the vast majority of potential e-Researchers. The future role out of Shibboleth across UK academia however offers an opportunity to align the Grid world and how internet resources are securely accessed more generally. Thus through authentication at a local identity provider, attributes certificates can be released which can subsequently be used by service providers to enforce authorisation decisions. The definition of and use of these dynamically allocated VO-specific attributes to enforce authorisation policies is thus aligned with the Shibboleth based approach. In addition, all of this is seamless and transparent to the end users of the system who simply log-in, typically to their own institution although depending on the scenario, they may log in to a virtual organisation specific identify provider.

A further indirect benefit of the work undertaken in DyVOSE was in training and educating future Grid engineers. Through DyVOSE the first Grid Computing course in the UK was established in 2004/5 at Glasgow, and one PhD student was tutored at Kent. Both are now in their third year. The PhD work has led to a number of research papers already being published with more in the pipeline. The lecture materials and more general course materials at Glasgow have been made freely available and have been adopted by several other Grid educators. The Grid Computing course at Glasgow formed the basis for technology development and its exploration through case studies in the DyVOSE project. Initially the focus was upon a static privilege management infrastructure where fixed policies were created to secure services implemented by the students as part of their advanced MSc within Glasgow. In the second phase of the project the focus was on dynamic privilege management infrastructures and focused on inter-organisational Grid security which exploited the DIS service.

The DyVOSE project has fully realised all of the objectives outlined in the project proposal and the results have been widely endorsed by the national and international Grid and Grid security communities. Testament to this is the large collection of publications generated through the project many of which were presented at the most competitive of international conferences. The project has also given numerous demonstrations and provided a range of talks at a range of fora across the whole e-Science spectrum. The project results are also making a direct impact on a variety of e-Research activities at the NeSC in Glasgow.

## Background

It has been suggested [1] that Grid-based research is typified by a “*me-Science*” culture, where the vast majority of people engaging and exploring the potential and benefits of Grid-based e-Research are those that are funded to do so. This is not the model foreseen at the outset of the UK e-Science core programme and is not a sustainable model. There are many reasons for this. One of the key factors is the existing model of security typified by mainstream Grids such as the UK National Grid Service (NGS) ([www.ngs.ac.uk](http://www.ngs.ac.uk)). With this model, end users are expected to obtain and manage an X509 certificate from the UK Certification Authority (CA) ([www.ngs.ac.uk/ca](http://www.ngs.ac.uk/ca)) which is used to support the Public Key Infrastructure (PKI) approach to access and usage of Grid resources. It is now accepted [2,3] that the experiences with public key certificates and PKIs for user authentication have not been too successful, and the PKI based approach of requiring end users to acquire and subsequently manage X.509 digital certificates is off-putting for less IT-savvy communities [4,5].

To help address this issue, it is an essential requirement that the potential e-Research community is provided with simple ways in which e-Resources can be accessed and used. Ideally, knowledge of the Grid and associated technologies should be kept at a minimum, especially for some less IT-oriented research domains/communities. Instead the emphasis should be on research generally and not on having to learn the intricacies of Grid infrastructures and their associated security mechanisms.

Furthermore, end users are not the only stakeholders in the e-Research domain that have issues with existing Grid security infrastructures. Resource providers are also reluctant (or at least wary) of offering their resources to the Grid where the security infrastructure is based upon an authentication-only type models. Thus knowing that a given digital certificate from a given user (identified by the Distinguished Name of their X.509 certificate) was used to install a virus program that crashed their system is not much use after the fact. Instead what are required are finer grained security models. These should allow resource providers or stakeholders such as managers at particular institutions to define their own security policies and enforce them locally in restricting (authorising) access to their own local resources, i.e. they should be completely autonomous. In this model, authenticated users are not given access to an account to do “stuff” but are provided with secure authorised access to specific services that can be invoked. These policies can be expressed in a variety of ways and resource providers can decide for themselves whether or not access to a resource should be provided (or not). Within the DyVOSE project we have explored how PERMIS can be used to both express security policies and subsequently enforce them when users (students) attempt to access and invoke Grid services.

One of the most important factors to consider when developing security technologies is usability. The best security infrastructures can be compromised in a variety of ways if usability is not addressed appropriately. For example, one of the primary sources of compromise is end users themselves whether maliciously or naively, e.g. through writing down their usernames and passwords. Thus the private key passwords associated with X.509 digital certificates as issued by the UK e-Science CA are required to be strong and consist of 16-characters with upper and lower case alphanumeric recommended. The temptation to write these down is thus tempting - especially when they are used sporadically. The result of this is that instead of increasing the level of security, it can be the case that the overall security is reduced.

The UK academic community is now exploring common models for access and usage of Grid based and non-Grid based resources through Shibboleth [6,7]. In the Shibboleth model, users attempting to access a protected service/resource (SP) will be redirected typically via a Where Are You From (WAYF) service to a known list of trusted identity providers (IdP). After selecting their home IdP and authenticating, the resource provider may – depending on the authentication information and privileges associated with that user, allow access to the resource. The UK Federation [8] has a small set of attributes which are supported and recognised based upon the *eduPerson* object class [9]. However this set of attributes will not address the demands of the rich range of application domains that the e-Science efforts have extended to. In this case disciplines need the flexibility to define their own domain specific or resource specific attributes and how they can subsequently be used to provide secure access to their resources to users in that community. In Grid parlance this can be interpreted as the ability to establish *virtual organisations* (VOs). VOs allow shared use of computational and data resources by collaborating users and institutions. Establishing a VO requires that efficient access control mechanisms to the shared resources by known individuals are in place. This can be done in a static manner where all resource providers and user communities agree in advance on the resources and users that will be accessing them, and in turn the security attributes that are needed to access those resources. However, to reflect the true vision of the Grid it is highly desirable to support dynamic establishment of VOs. It is in this context that the DyVOSE project has produced novel technologies and applied them across a range of disciplines. We note that the original target of application was on the education domain – specifically to support the teaching of Grid Computing at the University of Glasgow. However the scope and application of the technologies and DyVOSE project as a whole has extended to other domains thus indicating the applicability of the approach.

In the development of any new technologies for inter-organisational collaboration a crucial factor in their successful uptake is agreement and understanding ideally through agreed standards. DyVOSE builds on a body

of standardisation work in the area of authorisation: from the X.812 access control framework [10] and the X.509 standard [11] which standardised the certificates of a privilege management infrastructure (PMI). A PMI can be considered as being related to authorisation in much the same way as a PKI is related to authentication. Consequently, there are many similar concepts in PKIs and PMIs. An outline of these concepts and their relationship are discussed in detail in [12]. A key concept from PMI are attribute certificates (ACs) which, in much the same manner as public key certificates in PKI, maintain a strong binding between a user's name and one or more privilege attributes. The entity that digitally signs a public key certificate is called a Certification Authority (CA) whilst the entity that signs an AC is called an Attribute Authority (AA). The root of trust of a PKI is sometimes called the root CA – which in terms of the UK e-Science community is given by the Grid Support centre at RAL. The root of trust of the PMI is called the source of authority (SOA). CAs may have subordinate CAs whom they trust and to which they delegate the powers of authentication and certification. Similarly, SOAs may delegate their powers of authorisation to subordinate AAs. If a user needs to have their signing key revoked, a CA will issue a certificate revocation list. Similarly, if a user needs to have authorisation permissions revoked, an AA will issue an attribute certificate revocation list (ACRL). Typically, a given user's access rights are held as access control lists (ACLs) within each target resource. In an X.509 PMI, the access rights are held within the privilege attributes of ACs that are issued to users. A given privilege attribute within an AC will describe one or more of the user's access rights. A target resource will then read a user's AC to see if they are allowed to perform the action being requested.

The Privilege and Role Management Infrastructure Standards Validation (PERMIS) technology is an authorisation infrastructure that realises a PMI. Through PERMIS, an alternative and more scalable approach to centrally allocated X.509 certificates can be achieved through the issuance of locally allocated ACs. Prior to the DyVOSE project, the PERMIS infrastructure supported a *static delegation* of authority model. In this model a central authority had to be contacted, and register local managers in its policy, before managers were entitled to assign privileges to subordinates. A better and more scalable solution however (as developed within DyVOSE) is to support *dynamic delegation* of authority. With dynamic delegation of authority, local managers do not need to be registered, but instead they are given the privilege to delegate when they are first given privileges to use the system. Managers can then allocate privileges to subordinates (staff or students) as required, without having to contact the central authority first to get permission. Support for inter-institutional dynamic delegation is the cornerstone for scalable security focused VOs and has been one of the key focal points for DyVOSE.

## 1. Aims and Objectives

The overall aim of the project as described in the initial DyVOSE project proposal work plan was to explore how fine-grained security-driven VOs could be established based around the PERMIS technology. Initially the focus of the project was on static PMIs with the later project efforts focusing on dynamic PMIs exploiting dynamic delegation of trust. The context of application was education – specifically in teaching the Grid Computing module at the University of Glasgow. The teaching and associated programming assignments associated with these courses provided the basis for the explorations in the project. The advanced MSC at Glasgow began in September 2004 and is now in its third year.

In detail (and as outlined in the project proposal) the specific objectives of DyVOSE were to:

- Design Grid based educational case studies initially using static and subsequently using dynamic delegation based PMI
- Report on practical experiences and best practices in static delegation based PMI
- Develop software supporting dynamic delegation and authority recognition in PERMIS
- Produce user manuals and administrator guides on using and setting up and managing dynamic delegation infrastructures
- Report on practical experiences in using dynamic delegation infrastructures as part of e-Science education
- Provide a NMI release of PERMIS that supports dynamic delegation of authority

*These objectives were all met throughout the course of the project and the project results have been widely accepted by the national and international community.*

A few minor changes were made to how these objectives were realised however. For example, the attribute certificates and case studies in the first phase of the project were focused initially around the Condor pool at the University of Glasgow and not on ScotGrid ([www.scotgrid.ac.uk](http://www.scotgrid.ac.uk)) as originally planned. This was primarily due to the nature of the case studies defined and the fact that ScotGrid was a moving target, i.e. the ScotGrid cluster was continually extended and refined through the addition of new equipment and replacement of older throughout the lifetime of DyVOSE. A new £850k SRIF-3 funded cluster was procured and deployed mid-2006 to form the basis for the e-Infrastructure at the University of Glasgow.

## 2. Methodology

### *General Methodology*

The methodology used within the project was based upon the project partner areas of expertise combined with a close working relationship. The University of Salford/Kent<sup>2</sup> (hereafter we refer only to the University of Kent) were the technology providers; the National e-Science Centre at the University of Glasgow were the applications providers and source of requirements based on the educational case studies. The basic *modus operandi* of the DyVOSE teams was that the University of Glasgow defined requirements and scenarios based on the needs of the Grid Computing course (and eventually based on several other projects), and subsequently tested the various software releases from the PERMIS team realising these requirements. Extensive feedback on the software and its associated documentation including bug fixes was made throughout the course of the project. As an experiment we also got the advanced MSc students in 2004/2005 themselves to perform an assessment of some of the tools from the PERMIS team. For example, the students were asked to define a security policy (which was subsequently used within their programming assignment) with the PERMIS policy editor. Considerable feedback was generated on the general usability of this tool that was sent back to the PERMIS team (and subsequently incorporated into their enhancement tool). It should be noted that all students were able to create policies using this tool however some students suggested that the HCI aspects of the tool (explicitly coded to be suited to non-computer literate folk) should be removed. This was counter to the UCL experiences in making the tool easier to use for everyone!

This policy was then used in the larger programming assignment. Specifically the policy was for a GT3.3 service (*searchSortGridService*) which wraps a Condor based application (this service offers two Java based methods to search (*searchMethod*) and sort (*sortMethod*) a large (5MB) text file (the complete works of Shakespeare). The students themselves were split into groups (*studentteam1*, *studentteam2*) with the authorisation policy to ensure that method *sortMethod* could only be invoked by members of their student group and the lecturing staff, whilst method *searchMethod* could be invoked by everyone. This set-up was used to illustrate the use of Role-Based Access Control (RBAC), where users are allocated privileges based on what role they have been assigned rather than their local user credentials. The students were also requested to secure their service using GSI (which provides service based security, as opposed to PERMIS method based security). Performance aspects and benchmarks for the speed of the different systems were recorded by the students.

Through this approach a detailed exploration of the PERMIS tool family was made (including the Policy Editor and the Privilege Allocator). The usability of the OGF/GGF AuthZ SAML interface (see Standards section below) was documented as the mechanism to establish Policy Enforcement Points on a wide scale. The assignment made use of an LDAP server associated with the Policy Decision Points. Of the 16 students that took the course, several managed to complete it fully (with many others getting close to completion). Thus the basic way in which access to Grid services could be restricted (authorised) via PERMIS was shown thereby demonstrating the feasibility of PERMIS for static PMI. Results and experiences from this phase of the project were demonstrated at a variety of conferences and venues including the 2005 UK e-Science All Hands Meeting, the 2005 Cluster Computing and Grid conference and numerous other events/workshops.

The programming assignment associated with the 2005/2006 students focused upon the *dynamic* establishment and usage of a PMI in a bioinformatics related project and utilized the Delegation Issuing Service (DIS). It is noted in particular that the latter phase of the project required much more interaction between the teams with regard to setting up the DIS. Extensive emails and site visits by the technology providers at Kent and the researchers at Glasgow and Edinburgh were made to realise the scenarios for the DyVOSE phase-2 dynamic PMI case study.

The case study itself involved separating the students that took the Grid computing module into two different research teams: one team analyzing protein sequence data and the other analyzing nucleotide sequence data. The students were required to implement a Globus-based bioinformatics BLAST application [13] to perform the analysis, which was to run across a Condor pool located at NeSC in Glasgow. Before they could perform the analysis, the students were expected to develop a Grid client to retrieve the data from a PERMIS protected data service (*BlastData*) in Edinburgh. Depending upon the *team* that they were in, either protein or nucleotide sequence data<sup>3</sup> would be returned respectively. These data sets were then used as input to a Globus GT3.3 based Grid service which the students implemented locally at Glasgow. These services parallelized the BLAST application over the NeSC Condor pool. The students Grid BLAST services themselves were protected through PERMIS so that only members of the appropriate student team were able to invoke their respective BLAST services. The two different authorization policies were pre-defined and deployed in the local NeSC

<sup>2</sup> The PERMIS team lead by Professor Chadwick moved from the University of Salford to the University of Kent within the lifetime of the DyVOSE project. JISC were informed of these changes in DyVOSE reports/deliverables. This move did not require any changes to the overall planning of the project.

<sup>3</sup> Or no data if neither of these roles were presented.

LDAP server by the teaching staff. The students were able to secure their Grid services through including the appropriate authorization policy in their deployment descriptor file.

In the initial implementation the *Edinburgh SoA* (Dr Jos Koetsier, DyVOSE RA in Edinburgh) used the Glasgow DIS service to issue attributes within the Glasgow PMI for the two roles (*EdTeamP* or *EdTeamP*) needed to gain access to the Edinburgh-based *BlastData* Grid service, i.e. the SoA was delegated the privilege by the *Glasgow Administrator* (Dr John Watt, DyVOSE RA in Glasgow) to assign subordinate roles within the Glasgow role hierarchy. In this scenario the *Glasgow Administrator* delegated the privilege to the *Edinburgh SoA* to issue attribute certificates to roles below *externalStudent*. With this model the service provider (here the Edinburgh *BlastData* provider) was able to select via the DIS which users (from Glasgow) should be allocated the specific role needed to access and use his service. In this model, the Edinburgh service provider has fine grained control of the attributes and specific users who should be given them. For smaller tightly controlled VOs, this model might be beneficial. For larger scale VOs however it might be better for the service provider to simply delegate this responsibility to an appropriate remote administrator, e.g. in this scenario the Grid computing course director at Glasgow might be delegated the privilege to issue *EdTeamN/EdTeamP* roles to students at Glasgow. Both of these scenarios are fully supported by the DIS and have been explored in DyVOSE.

Through creation of a VO specific role within the Glasgow role hierarchy by the *Edinburgh SoA*, Glasgow students were subsequently able to access and return the appropriate sequence data sets for input to the BLAST service. Of the 11 students that undertook the Grid Computing module and associated programming assignment in 2005/2006, several successfully completed all of the assignment. All of the students that built the Grid client were able to return data from Edinburgh. As such, this education domain application of the DIS showed the proof of concept for how a service provider (*BlastData*) could either securely create or make use of dynamically issued attribute certificates at remote sites to subsequently allow for fine grained authorization decisions on their resource. Papers and live demonstrations of this system have been made at a variety of fora including the 2006 UK e-Science All Hands Meeting, the e-Science 2006 conference, the Cluster Computing Grid conference and many other events/workshops. (See attached papers for details of these experiences).

We note that once established the DIS provides a direct way in which delegation of authority supporting role assignment and its use in enforcing authorization decisions can be achieved. As mentioned, the team at Glasgow and Edinburgh worked extensively with the researchers at Kent in deploying and configuring the DIS service. Key to this whole process is documentation. The DyVOSE teams have now developed extensive documentation outlining the many steps that are involved in installing, configuring and subsequently using the DIS. This information is available both on the DyVOSE web site and as an attachment to this report.

### **Standards**

The PERMIS team work closely within the international standards community including bodies such as ITU-T as well as the Open Grid Forum (OGF) - previously known as the Global Grid Forum (GGF). Indeed Prof Chadwick is chair of the OGF/GGF Authorisation working group. The PERMIS technology itself was the first implementation of an X.509 compliant role-based Privilege Management Infrastructure (PMI).

The PERMIS technology also supports the OGF/GGF SAML AuthZ callout application programming interface which provides a policy enforcement point (PEP) with a standard way of utilising an arbitrary authorisation infrastructure. The Grid specification is an enhanced profile of the OASIS Security Assertion Markup Language (SAML) v1.1 which defines a number of elements for making assertions and queries regarding authentication, authorization decisions and attributes. The OASIS SAML AuthZ specification defines a message exchange between a policy enforcement point (PEP) and a policy decision point (PDP) consisting of an *AuthorizationDecisionQuery* flowing from the PEP to the PDP, with an assertion returned containing some number of *AuthorizationDecisionStatements*. The *AuthorizationDecisionQuery* itself consists of: a Subject element containing a *NameIdentifier* specifying the initiator identity; a Resource element specifying the resource to which the request to be authorized is being made, and one or more Action elements specifying the actions being requested on the resources. The OGF/GGF SAML profile specifies a *SimpleAuthorizationDecisionStatement* (essentially a granted/denied Boolean) and an *ExtendedAuthorizationDecisionQuery* that allows the PEP to specify whether the simple or full authorization decision is to be returned. In addition the GGF query supports both the pull and push modes of operation for the PDP to obtain attribute certificates, and has added a *SubjectAttributeReferenceAdvice* element to allow the PEP to inform the PDP where it may obtain (pull) the subject's attribute certificates from.

Through this SAML AuthZ API, a generic PEP can be built which can be used to protect arbitrary Grid services. Thus rather than developers having to explicitly engineer a PEP on a per application basis, the information contained within the deployment descriptor file (.wsdd) when the service is deployed within the container, is used to configure the generic PEP. Authorisation checks on users attempting to invoke "methods" associated with this service are then made using the information in the .wsdd file and the attributes contained in the LDAP repository together with the DN of the user themselves extracted from their X.509 user certificate.

Note that this “method” authorisation basis extends current security mechanisms such as GSI which work on a per service/container basis. This generic solution can be applied to numerous infrastructures used to realise PDPs such as PERMIS. Within DyVOSE, Globus toolkit (GT3.3) and PERMIS were used as they both supported this API. Since then other implementations of this API have been implemented, e.g. the WSRF.net work at the University of Virginia [14]. Later releases of Globus (GT4) have also supported this API.

One issue that was encountered with the SAML AuthZ profile within DyVOSE was the lack of granularity in how users might invoke actions. For example, different actions may or may not be allowed depending upon the data that they wish to access and potentially change. The SAML AuthZ profile does not currently allow actions to be distinguished based upon the parameters that might be associated with them. As a result, Grid services cannot for example have authorisation policies dependent upon specific data sets in a database appropriate to an invoker. Instead, the SAML AuthZ specification supports either a secure Grid service or a non-secure Grid service. In short, it is not possible to distinguish the usage of individual operations, e.g. to allow arbitrary invocations of actions where the data sets themselves are parameters of the actions and might change.

The OGF/GGF community are now working on extensions to this SAML AuthZ profile to address these limitations.

The DIS service within DyVOSE allows for the definition and subsequent use within authorisation infrastructures of arbitrary project (VO-specific) attributes. The model of definition and subsequent usage of attributes hosted by institutions is very much aligned with the model of Shibboleth access and usage within the wider UK academic and international communities. Thus for example, the UK Federation recommends a core set of attributes based around the *eduPerson* object model. Specifically these include: *eduPersonScopedAffiliation*: which indicates the user’s relationship (e.g., staff, student, etc.) with the institution; *eduPersonTargetedID*: is needed when an SP is presented with an anonymous assertion only, as provided by *eduPersonScopedAffiliation*. In this situation it cannot for example provide usage monitoring across sessions. The *eduPersonTargetedID* attribute provides a persistent user pseudonym; *eduPersonPrincipalName*: is used where a persistent user identifier, consistent across different services, is needed; *eduPersonEntitlement*: enables an institution to assert that a user satisfies an additional set of specific conditions that apply for access to a particular resource. A user may possess different values of the *eduPersonEntitlement* attribute relevant to different resources.

Each of these attributes can be used to provide the necessary information to service providers to make authorisation decisions. These attributes are versatile and likely to be sufficient for the great majority of applications. It is important to note that these attributes are statically defined and agreed upon between the institutions prior to formulation of VOs or requests to access Grid resources, i.e. they are based upon statically defined PMIs. The DyVOSE DIS service provides a complementary approach whereby bespoke attributes can be defined and used to enforce authorisation decisions in a much more dynamic manner.

Numerous on-going projects at the National e-Science Centre at the University of Glasgow have shown how a large range of research driven VOs can be accessed and used through the single sign-on capabilities of Shibboleth. Multiple presentations and demonstrations of these systems have been made.

### 3. Implementation

The work was undertaken in accordance with the work plan identified at the beginning of the project and as indicated in the previous section. Regular updates of project progress were provided to JISC throughout the course of the project. There were no major deviations from the course of the project plan. One minor deviation was due in part to the success of the project as a whole. That is, the life time of the project was (generously) extended by JISC for a further six months to support intellectual transfer of project results. This was due to the widespread dissemination of project results (see section 5 below) at a variety of conferences and workshops.

We note that whilst it was not planned that others would use the pilot testing results, we have taken extensive steps to ensure that further use of them is possible. For example, we have put extensive documentation together on all aspects of defining security policies and linking them to Grid services supporting the OGF/GGF SAML AuthZ callout; on how to set up and use the DIS. Ideally of course the true benefit from the project and its uptake can only really be measured by others who have followed these various documentations and managed to successfully establish their own protected Grid resources. This has not yet happened. Although we note that we plan to explore precisely these kinds of scenarios through our involvement in the OGC Grid Collision project [15] with EDINA.

We also note that even with very detailed documentation, the knowledge required to fully exploit the DyVOSE results is extensive. Through NeSC involvement in projects such as ESP-Grid with the University of Oxford, it was apparent that the low level implementation details required for example to configure Grid systems, authorisation infrastructures and Shibboleth systems cannot easily be transferred without direct hands-on support. It is not clear how this can be resolved. There is no simple silver-bullet that can support the various flavours of Grid middleware, and its relationship to various authorisation technologies such as PERMIS and combining them with Shibboleth. It is a complicated space and it would be naïve to pretend otherwise. We have

shown how such technologies can be integrated based upon specific versions of technologies with specific scenarios in mind. As it seems with most of the Grid based solutions right now, there is still a great deal of dependencies on different flavours of operating systems and how the various technologies themselves have been deployed and configured. The best that we are able to achieve is to describe how we have successfully defined these technologies and show that it can be done if a particular recipe is followed, i.e. document how it can be done in detail. As noted however this documentation requires very low level understanding of combinations of technologies and this may well be beyond the normal experience/know-how of arbitrary users or administrators. A proposal to JISC on the longer term take-up of these results by others across Scotland and beyond (TIGERS) identified these many issues in detail but ultimately was not funded.

The nature of the case studies and how the work was implemented as a whole was described in section 2.

## 4. Outputs and Results

The project has produced many different kinds of output. These have included:

- Dynamic delegation of authority software through extensions to the PERMIS technology. The software manifest includes: a standalone Delegation Issuing Service (DIS), a web server front end to the DIS accessible via standard web browsers, enhancement to the PERMIS Policy Editor to support delegation policies, and enhancements to the PERMIS PDP/CVS to support the dynamic fetching and validation of delegated chains of credentials;
- lecturing, teaching and training materials on all aspects of Grid education;
- a PhD student who is now writing up his thesis on dynamic delegation of authority
- a variety of scenarios reflecting future Grids requirements for establishment of VOs based upon static and dynamic PMI;
- in depth experiences on the establishment and exploitation of Grid and related technologies including insights into when it is useful to exploit Grid technologies (e.g. for performance considerations) and when not based on a variety of different benchmarking;
- a collection of Grid services, portals and range of capabilities demonstrating the applicability of the solutions put forward in DyVOSE.
- a multitude of papers and demonstrators highlighting the results of the project as a whole;

Some of the more significant papers are attached with this report. We would also refer the reader to the numerous case studies described in these papers with regards to how the systems have been established and how fine grained access control on a per-VO basis has been achieved.

Earlier demonstrations of the Shibboleth enabled access to portals and systems contained therein are described in detail in [http://wiki.oucs.ox.ac.uk/esp-grid/NeSC\\_Shibbolized\\_Resources](http://wiki.oucs.ox.ac.uk/esp-grid/NeSC_Shibbolized_Resources) (through the work undertaken in the ESP-Grid with the University of Oxford);

A demonstration of the project results in the form of slides demonstrating the capabilities and running of the DIS given as an attachment to this report (see DISdemo.pdf). These slides indicate the steps involved in starting and using the DIS as well as the various snapshots of what happens when security attributes are allocated (with access being granted/or not depending on the possession of specific attributes).

The single sign-on and use of VO-specific attributes and their support for fine grained authorisation and single-sign on with Shibboleth are presented in (VOattributesandShibSSOinLifeSciences.pdf) also given as an attachment to this report. These slides demonstrate how the VO-specific attributes across the life science domain can be used to gain secure (authorised) access to a variety of VO-specific Grid resources accessible via portals. These are based on neurological case studies and bioinformatics applications, however a variety of other scenarios in other domains have also been supported with other on-going projects also exploiting the results of DyVOSE.

The actual publications generated from the project itself are:

R.O. Sinnott, D.W. Chadwick. *Experiences of Using the GGF SAML AuthZ Interface*, Proceedings of UK e-Science All Hands Meeting, September 2004, Nottingham, England.

R.O. Sinnott, A.J. Stell, D.W. Chadwick, O.Otenko, *Experiences of Applying Advanced Grid Authorisation Infrastructures*, Proceedings of European Grid Conference (EGC), LNCS 3470, pages 265-275, Volume editors: P.M.A. Sloot, A.G. Hoekstra, T. Priol, A. Reinefeld, M. Bubak, June 2005, Amsterdam, Holland.

R.O. Sinnott, A.J. Stell, J. Watt, *Experiences in Teaching Grid Computing to Advanced Level Students*, Proceedings of CLAG+Grid Edu Conference, May 2005, Cardiff, Wales.

A.J. Stell, R.O. Sinnott, J. Watt, *Comparison of Advanced Authorisation Infrastructures for Grid Computing*, Proceedings of International Conference on High Performance Computing Systems and Applications, May 2005, Guelph, Canada.

- J. Watt, R.O. Sinnott, A.J. Stell, *Dynamic Privilege Management Infrastructures Utilising Secure Attribute Exchange*, Proceedings of UK e-Science All Hands Meeting, September 2005, Nottingham, England.
- D.W.Chadwick, *Delegation Issuing Service* in Proceedings of the NIST 4<sup>th</sup> Annual PKI Workshop, Gaithersberg, USA, April 19-21 2005, pp 62-73 (available from [http://middleware.internet2.edu/pki05/proceedings/chadwick-delegation\\_issuing.pdf](http://middleware.internet2.edu/pki05/proceedings/chadwick-delegation_issuing.pdf))
- R. O. Sinnott, M. M. Bayer, J. Koetsier, A. J. Stell, *Advanced Security on Grid-Enabled Biomedical Services*, Proceedings of UK e-Science All Hands Meeting, September 2005, Nottingham, England.
- R.O. Sinnott, *Development of Usable Grid Services for the Biomedical Community*, Workshop on Designing for Usability in e-Science, Edinburgh, January 2006.
- R. O. Sinnott, M. M. Bayer, J. Koetsier, A. J. Stell, *Grid Infrastructures for Secure Access to and Use of Bioinformatics Data: Experiences from the BRIDGES Project*, 1<sup>st</sup> International Conference on Availability, Reliability and Security, (ARES'06), Vienna, Austria, April, 2006.
- J. Watt, R.O. Sinnott, O. Ajayi, J. Jiang, J. Koetsier, *A Shibboleth-Protected Privilege Management Infrastructure for e-Science Education*, 6<sup>th</sup> IEEE International Symposium on Cluster Computing and the Grid, CCGrid2006, May 2006, Singapore.
- R.O. Sinnott, A.J. Stell, O. Ajayi, *Development of Grid Frameworks for Clinical Trials and Epidemiological Studies*, HealthGrid 2006 conference, Valencia, Spain, June 2006.
- R.O. Sinnott, J. Watt, O. Ajayi, J. Jiang, *Shibboleth-based Access to and Usage of Grid Resources*, IEEE International Conference on Grid Computing, Barcelona, Spain, September 2006.
- R.O. Sinnott, O. Ajayi, A.J. Stell, J. Watt, J. Jiang, *Single-Sign on and Authorization for Dynamic Virtual Organizations*, International Conference on Virtual Enterprises, (PRO-VE'06), Helsinki, June 2006.
- R.O. Sinnott, A.J. Stell, J. Watt, D.W. Chadwick, *Advanced Security Infrastructures for Grid Education*, 10th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2006), Orlando, Florida, July 2006.
- A.J. Stell, R.O. Sinnott, O. Ajayi, *Supporting the Clinical Trial Recruitment Process Through the Grid*, Nottingham UK e-Science All Hands Meeting, September 2006.
- J. Watt, R.O. Sinnott, J. Koetsier, A.J. Stell, *DyVOSE Project: Experiences in Applying Privilege Management Infrastructures*, UK e-Science All Hands Meeting, Nottingham UK, September 2006.
- R.O. Sinnott, J. Watt, D.W. Chadwick, J. Koetsier, O. Otenko, T.A. Nguyen, *Supporting Decentralized, Security focused Dynamic Virtual Organizations across the Grid*, 2<sup>nd</sup> IEEE International Conference on e-Science and Grid Computing, Amsterdam, December 2006.
- A.J. Stell, R.O. Sinnott, O. Ajayi, *Secure, Reliable and Dynamic Access to Distributed Clinical Data*, Life Science Grid Conference, Yokohama, Japan, October 2006.
- R.O. Sinnott, O. Ajayi, A.J. Stell, J. Watt, J. Jiang, *User Oriented Access to Secure Biomedical Resources through the Grid*, Life Science Grid Conference, Yokohama, Japan, October 2006.
- David Chadwick, Gansen Zhao, Sassa Otenko, Romain Laborde, Linying Su, Tuan Anh Nguyen. *Building a Modular Authorization Infrastructure*, All Hands Meeting, Nottingham, September 2006. Available from <http://www.allhands.org.uk/2006/proceedings/papers/677.pdf>
- R.O. Sinnott, O. Ajayi, A.J. Stell. *Supporting Grid Based Clinical Trials in Scotland*, submitted to Health Informatics Journal, November 2006.
- David W Chadwick, Sassa Otenko and Tuan Anh Nguyen, *Adding Support to XACML for Dynamic Delegation of Authority in Multiple Domains*, Proc of 10th IFIP TC-6 TC-11 Int Conf, CMS 2006, Heraklion, Crete, Greece, Oct 19-21, 2006. Springer LNCS Volume 4237/2006, pp67-86.
- O. Ajayi, R.O. Sinnott, A.J. Stell, *Trust Realisation in Collaborative Clinical Trials Systems*, HealthCare conference, Harrogate, UK, March 2007.
- R.O. Sinnott, O. Ajayi, J. Jiang, A. J. Stell, J. Watt, *User-oriented Security Supporting Inter-disciplinary Life Science Research across the Grid*, to appear in New Generation Computing, Special Edition on Life Science Grids, editors A. Konagaya, P. Arzberger, T. W. Tan, R. Sinnott, D. Angulo, March 2007.
- O. Ajayi, R.O. Sinnott, A.J. Stell, *Formalising Dynamic Trust Negotiations in Decentralised Collaborative e-Health Systems*, 2<sup>nd</sup> International Conference on Availability, Reliability and Security, (ARES'07), Vienna, Austria, April, 2007.
- A.J. Stell, R.O. Sinnott, O. Ajayi, *Security Oriented e-Infrastructures Supporting Neurological Research and Clinical Trials*, 2<sup>nd</sup> International Conference on Availability, Reliability and Security, (ARES'07), Vienna, Austria, April, 2007.
- J. Watt, R.O. Sinnott, J. Jiang. *Applying Shibboleth Single Sign-On and Access Control to Cross-Campus Student Web Resources*, submitted to TERENA conference, Copenhagen, Denmark, May 2007.

R.O. Sinnott, C. Bayliss, J.Jiang, *Security-oriented Data Grids for Microarray Expression Profiles*, to appear in HealthGrid 2007 conference, Geneva, April 2007.

R.O. Sinnott, O. Ajayi, A.J. Stell, C. Bayliss, J. Watt, J. Jiang, *Supporting Life Science Research through Shibboleth and Community Grid Portals*, to appear in HealthGrid 2007 conference, Geneva, April 2007.

D.W.Chadwick. *Dynamic Delegation of Authority in Web Services*, chapter in book "Securing Web Services: Practical Usage of Standards and Specifications". Edited by Dr Panayiotis Periorellis, Newcastle Univ. to be published by Idea Group Inc. in 2007

## 5. Outcomes

The outcomes of the project are considerable. All of the aims and objectives at the outset of the project have been realised. The outcomes and experiences gained through DyVOSE have been of immense benefit to the NeSC in its role as a national co-ordinating centre for UK-wide e-Science efforts and promoting the take-up of e-Science more generally. The outcomes themselves have included gaining direct experiences with a rich variety of Grid middleware and setting it up for training purposes - as mentioned the NeSC at Glasgow established the first full Grid Computing course in the UK and the efforts required to achieve this were considerable especially for this first time in the fluid Grid landscape. These experiences have – as far as possible – been passed on to others. For example, we have been involved in NGS training events and given lectures at other sites (e.g. lectures on Grid security as part of the Edinburgh MSc in e-Science). We have also been involved in summer schools on application of Grid technologies. In addition we have been involved in the Open Grid Forum area of training and education to actively promote the Grid teaching efforts lead by the e-Science Institute in Edinburgh by Prof. Malcolm Atkinson and Dr David Fergusson.

The materials and experiences in educating future Grid developers have been extremely useful since it has allowed consolidating the experiences of on-going projects exploiting various Grid middleware. We note that teaching advanced MSc students in particular has been especially beneficial (and challenging!) since they are (for the most part!) experienced and quite savvy-software developers who have already built a variety of distributed systems through their undergraduate courses (a pre-requisite for enrolment on the Glasgow Grid Computing module). The Grid Computing course is now in its third year of running and the feedback from the students with regards to this course have been very positive – despite the multiple challenges that often arise with bleeding-edge Grid middleware.

Based on the portfolio of security related projects on-going at the NeSC at the University of Glasgow, the results and experiences from DyVOSE are directly shaping multi-disciplinary efforts. The example slides attached with this proposal give a feeling for the research that DyVOSE has provide the platform for. Furthermore through the JISC funded early adopter GLASS project, the ramifications of establishing a university wide identity provider for authentication combined with departmental servers providing VO-specific security attributes are shaping efforts in how best to exploit Shibboleth in the e-Research arena more generally.

Ideally of course, the true success of a project is when the results can be directly taken up and used by others. As noted previously, we have tried to actively support the promotion and exploitation of project results. It is still the case however that the knowledge and experience required across a heterogeneous range of software and middleware to support e-Research is considerable. The work undertaken within DyVOSE has provided NeSC with experiences that are irreplaceable and has provided a platform for numerous on-going projects. As stated, documentation is crucial to the successful uptake of software results, and we have taken considerable time to record the systems we have built and how they have been configured. Whether others will exploit the results of DyVOSE (as much as they are being exploited by NeSC) remains to be seen. However, it is clear that demonstrators showing Shibboleth based single sign-on across multiple different VOs where VO-specific attributes are defined and used to authorise access to and usage of VO-specific resources can only encourage the uptake of project results. Compelling institutions or projects to adopt such technologies with their associated complexities can only be achieved when direct results exist that prove that the technologies both work, and perhaps more importantly, that they support research infrastructures that meet real research needs.

## 6. Conclusions

The DyVOSE project has fully realised all of its objectives with advanced software rolled out and successfully applied to support both teaching at Glasgow, and a broad range of other e-Research at Glasgow. In addition one PhD student has been supervised. Indeed a sign of the success of the project is how it has grown in scope far beyond the basic education domain to encompass a large spectrum of other application areas where fine grained security is essential. These have included the biological domain and clinical trials domain through major projects funded by the BBSRC, DTI and MRC, with major EPSRC pilot projects planning to exploit the project results also.

The project has provided a platform through which the Shibboleth architecture and protocols could be explored to show how definition and assignment of attribute certificates and how they are subsequently used to enforce authorisation policy could be realised. Live demonstrations of single sign-on via Shibboleth where project (VO-specific) attributes are needed and used to enforce authorisation policies has been demonstrated at major events including the OGF/GGF to the Internet2 and wider Grid research communities, and numerous other UK and international Grid conferences and workshops such as UCISA.

The project has attempted as much as possible not simply to market its results through conferences, but in delivering hands-on expertise to others interested or attempting to get involved in this space. For example, presentations have been given at events organised by Middleware Assisted Take-Up project ([www.matu.ac.uk](http://www.matu.ac.uk)), at UCISA conferences for information managers/IT directors across UK academia. More direct support has also been offered. For example, the DyVOSE team realised the demonstrator for the JISC funded ESP-Grid at the University of Oxford which showed how Shibboleth could be used to transfer attributes needed to securely access Grid resources across a range of e-Research projects.

Exploiting Shibboleth to delivering project specific attribute certificates for single sign-on across a range of projects has numerous benefits. Allowing e-Researchers to access Grid resources simply by logging in to their own local identity providers is appealing (and a model more likely to engage the users rather than them having to obtain and use X.509 digital certificates with 16 character strong passwords). This model is underpinning over £20M of projects across Glasgow University involving NeSC. Thus we firmly believe that the project has been a great success in all respects.

## 7. Implications

The proof of concept systems demonstrating how dynamic definition of security attributes based upon delegation of authority can be realised and subsequently used to make authorisation decisions could have (is having!) great impact on how future e-Infrastructures can be supported. Whilst the NeSC in Glasgow have a body of experience gained from the project in using varieties of Grid middleware and integrating them with authorisation technologies and Shibboleth, it still remains a challenge as to how best others might gain from these efforts. There is no easy way (unfortunately) people can directly benefit from the results of the project without having to immerse themselves with a variety of different technologies, i.e. the project has not produced a CD that can be installed to set up Globus, Shibboleth, PERMIS, portal technologies etc etc. Rather the end users and administrators are still required to engage in detailed installation and configuration. That said, the NeSC at Glasgow are supporting the efforts of others in this area. For example in the EDINA Grid OGC Collision project exploring Grid and Shibboleth technologies in the Geographical Information System domain.

Ensuring that an institution in a Shibboleth federation can guarantee the authenticity of a user when accessing a remote resource is crucial to the overall principles upon which Shibboleth and Shibboleth federations are based. In short, institutions in a federation should *trust* one another. It is the case however, that users at larger institutions will likely have numerous usernames and associated passwords that are used to access a variety of services. Until recently this was the case at the University of Glasgow! However activities are currently well underway to roll out a unified user account management system based upon directory technology. This is being explored within the JISC funded Glasgow early adopter of Shibboleth (GLASS) project ([www.nesc.ac.uk/hub/projects/glass](http://www.nesc.ac.uk/hub/projects/glass)). To overcome the issue of multiple usernames/passwords the University of Glasgow is moving to a system that offers a more consistent representation of staff and students across multiple systems that will allow: timely creation/modification and deletion of accounts; an audit trail against central records; a single authority for services covering the whole university; password synchronisation; and the implementation of a rigorous password policy. To support this, the university is planning: a one to one representation between each user and their corresponding entry in the Human Resource/Registry database – the definitive sources for data; an agreed standard for unique identifiers for each user account; an agreed password policy; an agreed definition of department/faculty codes where user accounts should reside. This system is based upon the Novell nSure technology ([www.novell.com/solutions/nsure](http://www.novell.com/solutions/nsure)) and is currently being rolled out by University Services across the university. Thus for federations involving the University of Glasgow we hope to state with some confidence that we are able to authenticate users that are members of the university.

There are numerous possible extensions to the work undertaken within the DyVOSE project. Currently for example, a delegator will use the DIS to delegate to an individual, e.g. a local or remote trusted administrator. In some scenarios it might be preferable for delegation to take place automatically without any human involvement. This is the case in various projects at NeSC for example. Consider the scenario where a resource is accessed via a portal. If the resource trusts the portal to delegate its authorization tokens to users as directed by its delegation policy, then when a user accesses the portal and requests access to the resource, if the delegation policy says this is OK, the portal should be able to automatically delegate the correct credential to the user, and then forward the user's request to the resource. The resource will then be able to validate that the user has the correct authorization token before granting the user access. In this scenario, delegation takes place automatically by the portal, but the resource still validates that its delegation policy was correctly enforced by the portal before

granting access to the user. A proposal to JISC (*n-Tier Dynamic Delegation of Authority*) was submitted to develop precisely such an extension to the DIS.

PERMIS is just one of the authorisation technologies available today. One of the most common authorisation middleware that has considerable adoption is VOMS [16]. VOMS, in its own words is “basically a simple account database, which serves the information in a special format (VOMS credential). The VO manager can administrate it remotely using command line tools or a web interface”. Even though it is only a simple account database, the account management is well developed and numerous large scale projects have adopted the VOMS technology. However, whilst PERMIS allows to both define and enforce security policies, there is no implicit reason why authorisation decisions themselves cannot be based upon attributes from other non-PERMIS sources, i.e. from a VOMS server. Combining VOMS and PERMIS has many advantages as it will benefit from the widespread user base that have adopted VOMS, whilst benefiting from the finer grained authorisation decision capabilities offered by PERMIS. A proposal to JISC (*Integrating VOMS and PERMIS for Superior Grid Authorization*) was submitted to develop precisely such an integrated system.

The work on DyVOSE has shown how VO-specific attributes can be delivered from for example a Shibboleth Identity Provider and used to gain access to a VO-specific Service Provider. A recent NeSC project funded by the Open Middleware Infrastructure Institute ([www.omii.ac.uk](http://www.omii.ac.uk)) is also planning to develop a family of JSR-168 compliant portlets which will provide a potentially lighter-weight approach for integrating Shibboleth with Grid based portals such as GridSphere. Specifically we will develop portlets for scoping attributes (to streamline the subset of IdPs from whom a portal will accept user attributes); to provide a portlet offering similar capabilities to the DIS; for dynamic content configuration of the portal based upon the attributes returned and available Grid services, and a portlet offering capabilities similar to the ShARPE technology allowing configuration of the attributes released from an IdP. These are very much complementary to the work undertaken within DyVOSE. Once developed these portlets will allow other e-Researchers to easily establish and exploit the benefits of Shibboleth technologies without necessarily having to refer to advanced authorisation technologies which might be outside of their experience/knowledge. Rather, the authorisation will be based upon portal content and configuration, i.e. if they have the right security attribute they will see the portlet to invoke that service.

## 8. References

- [1] “Me-Science the New e-Science”, <http://www.gridtoday.com/grid/963514.html>
- [2] B. Beckles, A user-friendly approach to computational grid security, Proceedings of the UK e-Science All Hands Meeting, Nottingham, UK, September 2006.
- [3] R.O. Sinnott, O. Ajayi, A.J. Stell, J. Watt, J. Jang, *User Oriented Access to Secure Biomedical Resources through the Grid*, Life Science Grid Conference, Yokohama, Japan, October 2006.
- [4] JISC Authentication, Authorisation and Accounting (AAA) Programme Technologies for Information Environment Security (TIES), [http://www.edina.ac.uk/projects/ties/ties\\_23-9.pdf](http://www.edina.ac.uk/projects/ties/ties_23-9.pdf).
- [5] Whitten, A., and Tygar, J. D. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. Paper presented at the 9th USENIX security symposium, Washington, 1999.
- [6] Shibboleth Architecture Technical Overview, <http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf>
- [7] Shibboleth Architecture Protocols and Profiles, <http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-arch-protocols-latest.pdf>
- [8] UK Federation, <http://www.jisc.ac.uk/federation/>
- [9] eduPerson object class, [www.educause.edu/eduperson/](http://www.educause.edu/eduperson/)
- [10] ITU-T Rec X.812 (1995) | ISO/IEC 10181-3:1996, Security Frameworks for open systems: Access control framework.
- [11] ITU-T Recommendation X.509 (2001) | ISO/IEC 9594-8: 2001, Information technology – Open Systems Interconnection – Public-Key and Attribute Certificate Frameworks.
- [12] D.W.Chadwick, A. Otenko, E.Ball. “Implementing Role Based Access Controls Using X.509 Attribute Certificates”, IEEE Internet Computing, March-April 2003, pp. 62-69.
- [13] Basic Local Alignment Search Tool (BLAST), <http://www.ncbi.nlm.nih.gov/Tools/>
- [14] WSRF.net platform, University of Virginia, <http://www.cs.virginia.edu/~gsw2c/wsrif.net.html>
- [15] SEE-GEO, [http://www.jisc.ac.uk/whatwedo/programmes/eresearch\\_grid\\_ogc\\_collision/project\\_see\\_geo.aspx](http://www.jisc.ac.uk/whatwedo/programmes/eresearch_grid_ogc_collision/project_see_geo.aspx)
- [16] R. Alfieri, et al, Managing Dynamic User Communities in a Grid of Autonomous Resources, CHEP 2003, La Jolla, San Diego, March, 2003

## Appendixes

Please find attached (in zip file):

Slides demonstrating:

- Set up and Usage of DIS (DISdemi.pdf)
- Single Sign-On and VO-specific Attributes in Life Science Domain (VOattributesandShibSSOinLifeSciences.pdf)

Documentation on how to set up and configure the DIS (DISinstall.pdf)

Some of the key papers generated throughout the course of the DyVOSE project.