



University
of Glasgow

Watt, J. and Sinnott, R.O. and Jiang, J. and Doherty, T. and Stell, A. and Martin, D. and Stewart, G. (2007) *Federated authentication and authorisation for e-science*. In: APAC Conference and Exhibition, 8-12 Oct 2007, Perth, Australia.

<http://eprints.gla.ac.uk/7365/>

Deposited on: 10 September 2009

Federated Authentication & Authorisation for e-Science

J. Watt, R.O. Sinnott, J. Jiang, T. Doherty, A.J. Stell, D. Martin, G. Stewart

National e-Science Centre, University of Glasgow, Glasgow G12 8QQ, UK

`j.watt@nesc.gla.ac.uk`

Abstract

The Grid and Web service community are defining a range of standards for a complete solution for security. The National e-Science Centre (NeSC) at the University of Glasgow is investigating how the various pre-integration components work together in a variety of e-Science projects. The EPSRC-funded nanoCMOS project aims to allow electronics designers and manufacturers to use e-Science technologies and expertise to solve problems of device variability and its impact on system design. To support the security requirements of nanoCMOS, two NeSC projects (VPMan and OMII-SP) are providing tools to allow easy configuration of security infrastructures, exploiting previous successful projects using Shibboleth and PERMIS. This paper presents the model in which these tools interoperate to provide secure and simple access to Grid resources for non-technical users.

Keywords: e-Science, Shibboleth, Grid, authentication, authorisation

1 Introduction

After years of consideration, the Grid community is now waking up to the limitations of its current security models. Collaboration and sharing of resources between e-Scientists has, up to now, been enabled by the creation of custom user accounts on the machines in question, irrespective of location, with access and protection given by X.509 digital certificates [1]. This inevitably leads to the situation where a user holds multiple user accounts on separately administered resources. As the number of Grid users grows, this decentralised model becomes unmanageable model and simply doesn't scale.

The National e-Science Centre (NeSC) at the University of Glasgow has focused on investigating tools to facilitate greater user uptake of Grid resources. Experience gained through NeSC projects like BRIDGES [2] have demonstrated that enticing novice users into adopting Public Key Infrastructures (PKIs) is at best difficult and at worst a severe risk. In general, the vast majority of e-Researchers do not wish to be Grid researchers. With this in mind, NeSC have worked primarily on development and deployment of portal and browser based technologies. By making services available through simple web interfaces, most of the complicated security interactions may be hidden from the end user, thus guarding the services against malicious use.

This paper provides an overview of how the 'back-end' security models are realised, hiding The Grid from e-Researchers and in turn making the overall system more usable and secure. The work draws on the results of several JISC-funded UK e-Science projects at NeSC [3], including the GLASS project (GLASgow early adoption of Shibboleth) [4] and the DyVOSE project (Dy-

dynamic Virtual Organisations for e-Science Education)[5]. Two current NeSC projects are aiming to extend these infrastructures to allow a complete security solution applicable to a wide variety of e-Research projects. The first project OMII-SP, aims to provide a set of portlets which allow easy configuration of portals exploiting Shibboleth and related security technologies. The second, VPMAN [6], is investigating integrating PERMIS and VOMS (Virtual Organisation Membership Service) [7] to take advantage of the complex features of the PERMIS authorisation decision engine along with the flexibility and compatibility of VOMS attributes. The proof of any middleware, or security technologies generally, ultimately depends on how they can be successfully applied. In this paper we focus on the security requirements of a major new e-Science project - “Meeting the Design Challenges of nanoCMOS Electronics” and illustrate how Shibboleth combined with results from the various NeSC security projects meets these requirements. All the projects mentioned above utilise a common set of middleware, all of which are designed to be generic solutions to the particular problems that they are addressing.

2 Technologies

2.1 Shibboleth

Shibboleth [8] is an Internet2 project which implements a federated authentication infrastructure currently based on SAML v1.1 [9], allowing a user’s home login credentials to be valid across a federation of trusted sites. In the

UK, the UKERNA Access Management Federation [10] provides a framework for Higher Education and Further Education institutions to recognise each others assertions of the identities of their own users. SAML (and therefore Shibboleth) defines a set of entities which interact in order to achieve this federated authentication model. A target or *Service Provider (SP)* represents a Shibboleth protected resource at a remote location and an origin or *Identity Provider (IdP)* provides information about its local users. A third entity, known as a *Where Are You From (WAYF)* service allows a user to select which institution (IdP) they belong to before authenticating.

Shibboleth is highly configurable with regards to the amount of user information that is disclosed to the federation. The individual entities keep track of a particular login session through the use of a temporary, non-identifying handle, effectively making identifying information optional within the SAML framework. At the other extreme, SAML supports the eduPerson [11] schema which allows a whole host of user information to be passed about. It is up to individual institutions and/or the federation itself to set the requirements for how much, or how little, disclosing information should be released to the federation. SAML attributes may be used to present user entitlements or *privileges* to providers, meaning that authorisation may be done using this information and not simply based on an authentication assertion.

Finally, the persistence of the user login session coupled with a non-identifying cookie means that Shibboleth may be used to implement a Single-Sign On (SSO) system, where a single login at the IdP represents authenticating to *ALL* services in the federation. As long as the browser window remains open this session will persist, and logging out of Shibboleth is as

easy as closing the browser window.

Considered from a Grid/e-Science paradigm, Virtual Organisations (VOs) will require users to authenticate at their home institution and various VO-specific attributes will be required to gain access to VO resources. Different models for storage of these attributes are possible. In the federated model, sites will support their own attribute authorities. In the centralised model (and the most common in mainstream Grids) a VO-specific attribute authority is established and used to define the roles and privileges for individuals in that particular VO. VOMS is often used for this very purpose - with an SP using these VO-specific attributes to make VO-specific authorisation decisions. One generic technology which enables all of the above models is PERMIS which may be used to protect nearly any kind of resource, and naturally has the ability to protect Grid resources running, for example, the Globus Toolkit.

2.2 PERMIS

PERMIS (Privilege and Role Management Infrastructure Standards Validation) is a set of software tools which allow Privilege Management Infrastructures (PMIs) [12] to be created which implement the X.812 generic authorisation framework [13]. The suite consists of a number of services which enable the issuance and maintenance of user credentials, the creation and enforcement of local security policies, and the interfacing of the PMI with numerous middleware and network services. PERMIS credentials take the form of X.509 Attribute Certificates (ACs) in which extra information about

the user's privileges on resources is stored. These privileges are usually expressed in the form of user roles within a VO, so method-level Role Based Access Control (RBAC) [14] may be used to secure access to resources. The ACs issued to users are digitally signed by an Attribute Certificate Manager (ACM) tool to prevent tampering, and may be loaded into an LDAP server or database so the user need not ever have to handle the certificate themselves. The privilege information contained within the AC typically refers to the user's *role* in an VO (e.g. 'student', 'administrator', 'consultant'), with the meaning of these roles being defined in the local VO-specific security policy. This policy is written by the resource or VO administrator, and contains complete information about the actions that may be performed on their resource, and the roles that are required to be held by a user in order to perform that action. The policy is also digitally signed and typically loaded into the administrator or 'Source of Authority' (SoA) entry in the LDAP server.

There exists a set of advanced tools for setting up PMIs with PERMIS. A Secure Audit Web Service [15] is available which allows a complete record of an institution's attribute use to be collated. This is useful for permanent records, but also to allow so-called 'Separation of Duty' checks to be made, where a user may be restricted in asserting attributes with conflicting privileges (e.g. being a 'student' AND an 'assessor' in the same examination).

The PERMIS Delegation Issuing Service (DIS) is a Web Service which is used to issue ACs to users. The DIS offers a number of advantages over the normal certificate issuing tool (ACM). The first being that any AC issuance is checked against the local XML security policy, meaning that ONLY

valid ACs can ever be issued. The second and most powerful feature is that it implements Dynamic Delegation of Authority, where the privilege to assign attributes (and issue ACs) relevant for access to a local resource may be delegated safely to subordinate users in your institution or to remote trusted individuals at remote institutions. This is effectively done by the administrator issuing a Role Allocation Policy (RAP) to the delegated user, which specifies which attribute(s) they may assign, their timescale, and also whether or not this delegated user may delegate the ability to assign these attributes even further down the chain. In a normal PKI chain of trust, this model runs into problems if an intermediate user has their signing key revoked, causing any ACs they signed to become invalid even though the privilege they granted is correctly assigned and still valid. The DIS avoids this issue by signing the certificate using its own PKI key-pair *on behalf* of the delegating user, so the removal of a rogue user who has issued an AC to a subordinate will not affect the validity of the AC because the AC was never signed by the rogue user - it was only issued by them, in accordance with the local policy.

Through DIS, the concept of dynamic delegation can be extended across institutions, effectively merging the capabilities of distinct PMIs. By recognising a collaborating institution's authority to sign attributes, the RAPs can be handed to any PMI, allowing attributes required for access to non-local services to be stored at the user's home institution. The credentials may also be stored at the resource side as well, although this will require an entry for the home user in the remote LDAP which may not be possible.

3 Scenarios

At NeSC we operate our own Shibboleth Identity Provider, which extracts static identifying information about its users (common name, jpegPhoto, organisation etc) from a central LDAP server. In the GLASS project, we are working with University IT Services to provide campus-wide authentication of students and staff. This is based on the roll-out of the Novell Nsure account management system, which will register all valid staff and students on their centrally managed LDAP-based database, and will involve the issuance of a unique ‘uid’ to each member which may be used to uniquely identify them within the institution. Since VO-specific authorisation attributes required to access local and remote resources are unlikely to be stored in a central LDAP, we have utilised the JNDI connectors in the Shibboleth attribute resolver to search multiple LDAP servers (departments) for user attributes. So, providing the departmental LDAP can link a user entry to the central LDAP via the unique ‘uid’ attribute, the department itself can issue the roles required for access to their own resources without having to go through some centralised attribute assigning process. Indeed this assigning needs no special software, just a normal LDAP browser is enough to assign these attribute strings. Figure 1 shows the interactions necessary to extract a complete campus attribute set.

Since the authentication step is performed at the central LDAP server, no matter how many attributes the user holds in each department, if the user’s privileges are removed - for example, if they leave the university having graduated (or having been thrown out!) they can no longer assert their

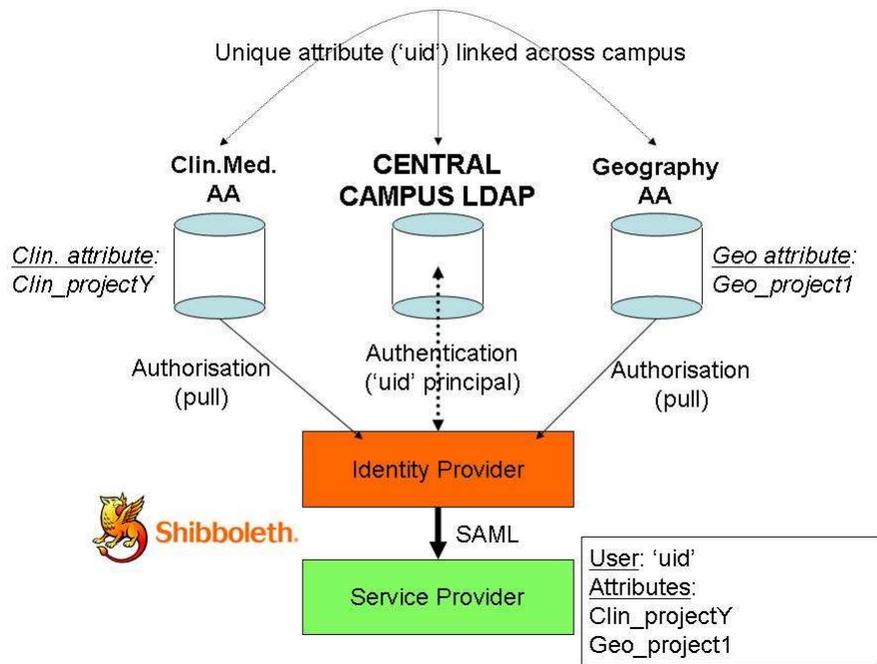


Figure 1: A schematic of distributed Attribute Authorities within a single institutional Identity Provider. Note that the attribute set that the IdP asserts is the union of the two departmental AAs.

identity in the federation and their attributes are not available for access. Distributed attributes within the domain of a single IdP is an ideal solution for campus level access control and single sign-on, however when dealing with a federation of IdPs there needs to be some way of assigning and also restricting the attribute set that visible to Service Providers. The assigning of attributes will probably involve a solution either outside of Shibboleth or integration with external applications. Restricting the attribute set seen by an SP are one of the goals of the OMII-SP Project. The OMII-UK [16] institute is aiming to provide a set of supported tools which will allow UK e-Science projects to share software and experience.

We note that these technologies are not directly dependent on the Grid middleware. The OMII-SP project is targeted to protection of OMII services, but the acceptance and restriction of VO-specific attributes can be equally applied to Globus services, for example, or Web Services more generally.

4 OMII Portal Services

One of the problems with joining a large Shibboleth federation of collaborating sites is that by agreeing to recognise the authentication assertions of remote institutions, without careful configuration you may find your resources are accessible by a far greater user set than you initially had intended. Indeed, with the out-of-the-box Shibboleth installation not using attributes for authorisation decisions, anyone within the federation who has successfully authenticated may access any Shibboleth protected resource within the federation. To counteract this, the use of Shibboleth SAML attributes can allow role-based access control to be enforced. However, if the attribute required for access is discovered by another institution outwith the collaboration, they may be able to present that attribute within their valid Shibboleth session and gain access. A simple way to prevent this is to utilise attribute scoping, where an attribute has additional location identifying information appended to it making it globally unique. For example, in the eduPerson schema, there is an attribute *eduPersonTargetedID* which is intended to be a locally unique, non-identifying attribute used for stateful services to retain profiles for returning users. If by accident two institutions assign the same *eduPersonTargetedID* to different users, then access to the other users de-

tails may become possible. Scoping the *eduPersonTargetedID* attribute can be done by appending the domain of the Identity Provider to the attribute. For example, if a user from Glasgow had the unscoped *eduPersonTargetedID* of ‘652425437’, the *scoped* attribute would be ‘652425437@gla.ac.uk’. This scoped value makes the locally unique unscoped attribute globally unique within the federation, guaranteeing it only refers to one person, a good analogy being the uniqueness of standard email addresses.

For Service Providers, it is important that one can discriminate between an institution you trust to assert your attribute and one that you only wish to trust the authentication assertions of its own users. In Shibboleth, this distinction is made by altering the Attribute Acceptance Policy (AAP). The AAP lists which attributes are accepted by the Service Provider, and from which sites these attributes will be trusted. Direct editing of the AAP is not trivial, and an error in the syntax could compromise the Service Provider.

Within the OMII-UK framework, the NeSC OMII-SP project is developing a family of JSR-168 compliant portlets that may be deployed in an environment like GridSphere. The first of these allows correct editing of the AAP using a intuitive GUI. It is worth noting a similar tool exists for editing of Identity Provider Attribute Release Policies called ShARPE [17]. Figure 2 shows the SCAMP (SCoped Attribute Manager Portlet) portlet interface, where trusted sites may be added or removed, and the form of the incoming attributes may be checked/scoped. For example, a particular VO like nanoCMOS may only wish to accept attributes which begin with ‘nanoCMOS_’. The portlet would normally only be accessible to the site administrator or a trusted delegate, and this access control can be enforced by

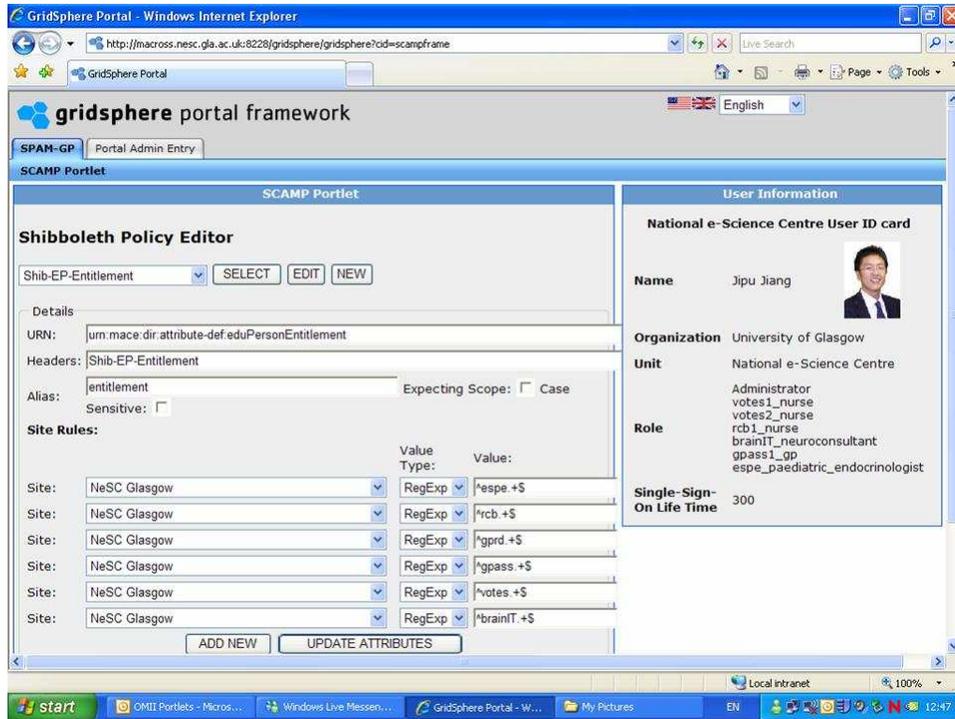


Figure 2: The SCoped Attribute Manager Portlet (SCAMP)

another Shibboleth attribute. On pressing the ‘publish’ button, the portlet commits this policy to the Shibboleth installation, and any new login sessions would be bound by the new rules. The software is currently at the testing phase, prior to adoption by the OMII Middleware group.

5 The nanoCMOS Project

The UK Engineering and Physical Sciences Research Council (EPSRC) Project nanoCMOS [18] is a collaboration between academia, leading electronics design houses, vendors and manufacturers to apply the knowledge of the e-Science community to some of the fundamental problems facing nanoCMOS

design [19]. In particular, the impact of transistor variability on overall circuit designs is a fundamental issue for the semiconductor industry for the next decade. The project is investigating the use of e-Science technology to allow geographically separated collaborators to interact with the overall design chain, with security for the intellectual property of the collaborating industrial partners a major priority.

The Grid jobs will be submitted to resources such as the National Grid Service [20] or more local resources like ScotGRID [21]. Authentication is levered primarily by X.509 proxy certificates, issued by the UK e-Science Certificate Authority [22], with authorisation done either through the use of gridmap files, or using VOMS attributes appended to the proxy certificate. Also in use in the UK is MyProxy [23] which allows a central repository to issue proxy certificates to its registered users. The widespread use of these current systems in the UK mean that any security solution will have to accommodate some if not all of them.

The first issue that needs to be resolved is the position of Shibboleth in this infrastructure. Shibboleth is an excellent SSO solution that allows federated authentication, but for institutional level IdPs, without some way of loading attributes intended for fine-grained access to external systems into the local IdP (or other attribute authority) it would only be possible to hold attributes intended for local access. In a distributed collaborative environment this is unworkable. However, if the Shibboleth attributes are considered only a part of the authorisation process, then these locally assigned attributes may be used to gain initial access to remote resources. So using the multi-Attribute Authority scenario described in the section above, a user

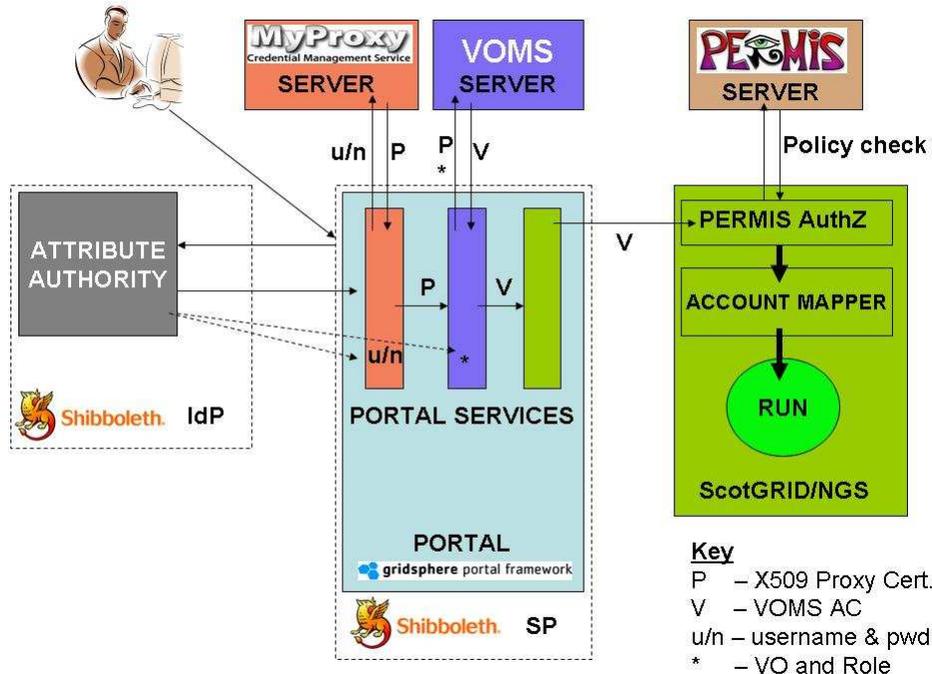


Figure 3: A diagram showing the interactions of the separate infrastructures within the nanoCMOS project.

who requires access to the front nanoCMOS page for which a ‘nanoCMOS’ attribute is required would visit their home department administrator who would load this attribute into their LDAP server. The attribute combined with the successful authentication would be enough to get an initial view of the page, but any actions on that page would be protected by further required credentials such as ACs. If these attributes are only for coarse-grained access control then institutions are less likely to refuse to distribute them across the federation, indeed they may be adopted as standard attributes in the same way as *eduPersonAffiliation* - so when a project receives funding it could be allocated an *eduPersonEntitlement* value that the relevant departments

within institutions may load into their local LDAP servers for each of the required users. This value could be a simple text name, or could be a hash or encrypted value to make it less revealing.

Figure 3 shows the interaction of the various components in the project. Once Shibboleth authenticated, an attribute-filtered view of the portal shows the services available to the user. At this point the user will need to invoke some Grid credentials to run jobs on external resources, in the UK this is a X.509 proxy certificate. MyProxy allows a user to activate a proxy certificate without passing the original certificate around. The username and password required may be input manually open login, or can be transported as a scoped Shibboleth attribute. The VOMS service allows the user to request a certificate asserting certain role/membership values, and these VOMS-specific attributes are appended to a user's X.509 credential. These values may be manually requested by the user, or they may also be extracted from local Shibboleth attributes. These credentials are recognised by the National Grid Service, so may be used to extract any other credentials that they demand for authorisation. These credentials may be used to map users into the correct environment for their project. This model can be applied to any major e-Science project utilising access to large-scale Grid resources.

6 Summary

NeSC have combined experiences of several of their projects to enable a security solution for the nanoCMOS project. This involves a Shibboleth Identity Provider which acts as an institutional level authentication mechanism based

on the GLASS project, which extracts service-specific user attributes from Attribute Authorities hosted at various departments on campus - a model which enables departmental project-level control of user attributes, but campus wide control of authentication assertions. This information is used to tailor a portal view that represents the user's abilities or privileges on the project portal, with the SCAMP portlet from the OMII-Portlets project being used to scope incoming attributes to ensure resources are only being requested from the correct institution. Finally the VPMAN project is investigating proposed standards to allow a portal to use the DN information from Shibboleth to extract credentials from a VOMS server, and use the PERMIS decision engine to authorise access using these attributes, or to extract its own PERMIS Attribute Certificates which may have been dynamically delegated across institutions. This work demonstrates several standard Grid security solutions working together to allow easy and secure access to resources until a complete international standard has been defined. We note that these technologies are being applied across a range of e-Research projects at NeSC including clinical trials, epidemiological studies, bioinformatics amongst numerous others. Through exploiting the browser-based SSO of Shibboleth, e-Researchers can now 'roam' across different VOs, with the pushing and pulling of the attributes required for authorisation completely hidden from the end users (as are the authorisation decisions themselves). In essence, these security technologies provide the glue that allows interdisciplinary research to be conducted in a seamless and transparent manner. Finally we note that the SCAMP portlet is the first of several to be produced in the OMII-SP project, with attribute push and release portlets being developed.

Our ultimate goal is to make establishment and use of security-oriented e-Infrastructure easy and manageable for future VOs, admins and end-users alike.

References

- [1] R. Housley et al. “RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile” *IETF*, Jan (1999) <http://www.ietf.org/rfc/rfc2459>
- [2] Biomedical Research Informatics Delivered by Grid Enabled Services (BRIDGES) <http://www.nesc.ac.uk/hub/projects/bridges>
- [3] J. Watt, O. Ajayi, J. Jiang, J. Koetsier, R.O. Sinnott. “A Shibboleth-Protected Privilege Management Infrastructure for e-Science Education” *Proc. of the Sixth IEEE International Symposium on Cluster Computing and the Grid (CCGrid06)*, IEEE Computer Society Press, (2006) pp. 357-364
- [4] J. Watt, R.O. Sinnott, J. Jiang. “The GLASS Project: Supporting Secure Shibboleth-based Single Sign-On to Campus Resources” *To appear in Sixth UK e-Science All Hands Meeting, Nottingham* (2007)
- [5] J. Watt, J. Koetsier, R.O. Sinnott, A.J. Stell. “DyVOSE Project: Experiences in Applying Privilege Management Infrastructures” *Proc. of the Fifth UK e-Science All Hands Meeting (NeSC ISBN 0-9553988-0-0)*, Sep (2006) pp. 669-676
- [6] Integrating VOMS and PERMIS for Superior Secure Grid Management (VPMAN) <http://sec.cs.kent.ac.uk/vpman/>
- [7] L. dell’Agnello, R. Alfieri et al. “From gridmap-file to VOMS: managing authorization in a Grid environment” *Future Generation Computer Systems 21 (Elsevier Science BV)*, (2005) pp. 549-558
- [8] S. Cantor et al. “Shibboleth Architecture: Protocols and Profiles” *Internet2-MACE (Document ID: internet2-mace-shibboleth-arch-protocols-200509)* 10th Sep (2005) <http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-latest.pdf>

- [9] E. Maler et al. “Assertions and Protocols for the OASIS Security Assertion Markup Language” *OASIS (Document ID: oasis-sstc-saml-core-1.1)* Sep (2005) <http://www.oasis-open.org/committees/security/>
- [10] UK Access Management Federation *UKERNA* <http://www.ukfederation.org.uk>
- [11] The eduPerson Specification <http://www.educause.edu/eduperson>
- [12] D.W. Chadwick, A. Otenko. “The PERMIS X.509 Role Based Privilege Management Infrastructure” *Future Generation Computer Systems 19(2) (Elsevier Science BV)*, (2002) pp. 277-289
- [13] “Security Frameworks for open systems: Access control framework” *ITU-T Rec X.812 — ISO/IEC 10181-3:1996* (1995)
- [14] D.W. Chadwick, A. Otenko, E. Ball. “Role-Based Access Control with X.509 Attribute Certificates” *IEEE Internet Computing*, Mar-Apr (2003) pp. 62-69
- [15] W. Xu, D.W. Chadwick, A. Otenko. “A PKI-Based Secure Audit Web Service” *IASTED Communications, Network and Information and CNIS (Phoenix, USA)*, Nov (2005)
- [16] The Open Middleware Infrastructure Institute UK (OMII-UK) <http://www.omii.ac.uk>
- [17] Shibboleth Attribute Release Policy Editor (ShARPE) <http://federation.org.au/ShARPE>
- [18] Meeting the design challenges of nano-CMOS electronics (nanoCMOS) <http://www.nanocmos.ac.uk>
- [19] R.O. Sinnott, A. Asenov et al. “Meeting the Design Challenges of nanoCMOS Electronics: An Introduction to an EPSRC Pilot Project” *Proc. of the Fifth UK e-Science All Hands Meeting (NeSC ISBN 0-9553988-0-0)*, Sep (2006)
- [20] The National Grid Service (NGS) <http://www.grid-support.ac.uk/>
- [21] The Scottish Grid Service (ScotGRID) <http://www.scotgrid.ac.uk>
- [22] J. Jensen. “The UK e-Science Certification Authority” *Proc. of the Second UK e-Science All Hands Meeting (EPSRC ISBN 1-904425-11-9)*, Sep (2003) pp. 336-369

- [23] J. Novotny, S. Tuecke, V. Welch. “An Online Credential Repository for the Grid: MyProxy” *Proc. of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10)*, IEEE Computer Society Press, Aug (2001)