

JISC DEVELOPMENT PROGRAMMES

Project Document Cover Sheet

Final Report for the SHEBANGS Project

Project

Project Acronym	SHEBANGS	Project ID	
Project Title	Shibboleth Enabled Bridge to Access the National Grid Service		
Start Date	21/11/05	End Date	21/02/07
Lead Institution	University of Manchester		
Project Director	Stephen Pickles		
Project Manager & contact details	Dr Stephen Pickles, Email: stephen.pickles@manchester.ac.uk Address: Manchester Computing, University of Manchester, Kilburn Building, Oxford Road, Manchester, M13 9PL Tel: (0161) 275 5974, Fax: (0161) 275 0637		
Partner Institutions			
Project Web URL	http://www.mc.manchester.ac.uk/research/projects/shebangs		
Programme Name (and number)	Core Middleware – Technology Development		
Programme Manager	James Farnhill		

Document

Document Title	<i>SHEBANGS Final Report</i>		
Reporting Period			
Author(s) & project role	Stephen Pickles (PI) and Mike Jones (Lead developer)		
Date	14/6/06	Filename	SHEBANGS-Final-Report-1-0.doc
URL			
Access	<input type="checkbox"/> Project and JISC internal		<input type="checkbox"/> General dissemination

Document History

Version	Date	Comments
0.1	31/3/07	First full draft.
0.9	14/6/07	Release candidate.
1.0	29/6/07	Submitted to JISC programme manager.

SHEBANGS: Final Report

Mike Jones and Stephen Pickles
Manchester Computing
University of Manchester

June 2007

Table of Contents

Title Page — SHEBANGS: Final Report.....	2
Table of Contents	2
Acknowledgements.....	3
Executive Summary	3
Background.....	4
Aims and Objectives	4
Methodology	4
Implementation	5
Outputs and Results	6
Outcomes	12
Conclusions	13
Implications.....	13
Recommendations.....	13
References	14

Acknowledgements

SHEBANGS was funded by the JISC through the Core Middleware – Technology Development programme.

We are grateful to our colleagues Ning Zhang and Aleksandra Nenadic for their invaluable contribution to the SHEBANGS project; to the organisers of and participants in various security workshops where we were able to discuss SHEBANGS and profit from informed community feedback, especially the Federated Identity Workshop at the Open Grid Forum and the AAI Infoday hosted by SWITCH; and to numerous individuals for their support, advice and encouragement, especially David Chadwick, David Chaplin, James Farnhill, Jens Jensen, Ross McIntyre, Andrew McNab, David Spence and Erik Vullings. We also acknowledge the ShibGrid Project.

Executive Summary

As a result of the JISC's strategic investment in Shibboleth, we look forward to an environment in which a growing wealth of UK services will support Shibboleth protocols to refer users to their home institutions for authentication. The JISC also provides funding to the National Grid Service (NGS). The NGS relies on the Grid Security Infrastructure (GSI – essentially a Public Key Infrastructure with extensions to support delegation), as do most production Grids today. These two security infrastructures are disjoint. Bridging the gap is a matter of urgency.

The earlier U.S. project GridShib addressed the problem of allowing Grid services to obtain attributes from (modified) Shibboleth servers in order to facilitate authorization decisions. SHEBANGS, and our sister project ShibGrid,¹ seek to bridge the gap in the opposite direction, i.e. to allow Shibboleth-authenticated users to access the Grid. The specific, high-level scenario that SHEBANGS addresses is as follows. An end-user, belonging to an organisation that operates a Shibboleth IdP, wishes to access some NGS resources or services provisioned using NGS resources. Moreover, the end-user is assumed (a) not to possess a digital certificate of the kind normally required to access the NGS, (b) to have no training in Grid computing, (c) not to have installed any Grid client software, and (d) to belong to a Virtual Organisation (VO) that is recognised by the NGS and whose members inherit a right to use NGS resources. We believe that a solution to this problem will have high impact.

Our overall approach and architecture are essentially unchanged from the original proposal. At the risk of over-simplification, SHEBANGS has developed a Credential Translation Service (CTS) that translates Shibboleth credentials (which cannot be understood by the NGS) to (VOMS-extended) short-lived GSI credentials (which can), in a manner which enables the NGS to make a subsequent authorisation decision. We envisage a community model in which a VO is sufficiently well-founded to offer (for example, via a web portal) to its members services that are themselves enabled by the NGS. Hence the deliverables of SHEBANGS are aimed primarily at developers of community portals.

SHEBANGS has delivered a full implementation of the CTS, including *inter alia* a re-usable Perl module VOMS::Lite (which gives access to the essential – for our purposes – capabilities of VOMS² with a much reduced set of dependencies), and an on-line

¹ ShibGrid was funded by JISC under the same call. The reader is referred to the ShibGrid project web site [SHIBGRID] for more information.

² At the risk of getting ahead of our story, we owe the reader some explanation of the Virtual Organizations Membership Service. VOMS uses extended GSI proxy credentials that carry SAML assertions about a users' membership of one or more VOs. Thus a VOMS-aware service to make an authorisation decision based on VO membership alone, without requiring a prior relationship with the

demonstrator. The source of all the SHEBANGS software is available from the SHEBANGS project web site under a dual license scheme (either the Perl Artistic License or FreeBSD at the user's discretion). SHEBANGS has been disseminated at numerous workshops, and a paper [AHM07] has been accepted by the UK e-Science All Hands Meeting 2007.

Although SHEBANGS has proven that its approach is technically feasible, further work is still required in this area. Limited deployments are likely to occur in the context of normal NGS activities. However, a holistic rationalisation and integration of the outputs of SHEBANGS and ShibGrid is required to address a broader range of use cases than either can address alone; a preliminary analysis undertaken by SHEBANGS and ShibGrid participants informed the FUSINGS proposal, but this was unsuccessful. More discussion is needed to establish community consensus on the general topic of deployment scenarios (especially establishment of trust) in the context of the policy of both Identity Management federations (on the Shibboleth side) and Certification Authorities (on the Grid side).

Background

As a result of the JISC's strategic investment in Shibboleth, we look forward to an environment in which a growing wealth of UK services will support Shibboleth protocols to refer users to their home institutions for authentication. The JISC also provides funding to the National Grid Service (NGS), in the form of hardware and personnel at the four core nodes CLRC (RAL), and the Universities of Leeds, Oxford and Manchester. The NGS relies on the Grid Security Infrastructure (GSI – essentially a Public Key Infrastructure with extensions to support delegation through proxy certificates), as do most production Grids today. Whereas the size of the NGS user community is measured in hundreds [NGS STATUS], the potential size of the community supported by Shibboleth Identity Providers (IdP) can be estimated by the number of Athens [ATHENS] usernames today (more than three million). While it is reasonable to expect that the number of *direct* users of the NGS, who are prepared to care for their own UK e-Science certificates, will grow to thousands, it is likely that this will remain orders of magnitude smaller than the number of Shibboleth users. Therefore it is strategically urgent for the NGS to gain leverage from JISC's investment in a Shibboleth infrastructure.

SHEBANGS provides a method whereby the NGS, and services provisioned using NGS resources, can be made accessible to end users who lack UK e-Science certificates of their own.

Aims and Objectives

The aim of SHEBANGS was to develop a bridge to enable a user authenticated by a trusted Shibboleth IdP to acquire (or delegate) temporary credentials to access resources on the National Grid Service.

Methodology

A minimalistic approach was sought whereby a service would be placed between other existing well established services without the need for integration. The purpose of this service would be to *translate* identity assertions provided from an unaltered Shibboleth IdP into GSI and VOMS credentials passed (delegated) to an unaltered MyProxy server for consumption by an unaltered grid portal. The method assumes a user to be equipped only with a standard web browser with no need for any knowledge of the intricacies of grid authentication and authorisation methods.

The development process was focussed upon the creation of a self contained middleware component so as to be highly portable. It was also decided that the need to rely upon

user. VOMS (and related software) come from the EGEE project. VOMS is used by many production Grids including the NGS and is key to solving the authorisation part of the SHEBANGS problem.

heavy-weight software such as that provided by Globus, LCG or gLite would hinder the uptake of this system and where possible these should be avoided. The focus was therefore placed upon the protocols used rather than the native APIs of the existing middleware. The resulting code was written assuming the environment required to set up a Shibboleth Service Provider (SP), i.e. an Apache Web server.

Implementation

The overall approach and architecture of SHEBANGS are essentially unchanged since the submission of the original proposal (see e.g. Figure 1). The main component of the SHEBANGS solution is the *Credential Translation Service (CTS)*. We have taken pains to make the CTS light-weight and portable. The CTS has been produced as a Perl module – VOMS::Lite – which can also be used outside the context of the SHEBANGS project and the Shibboleth environment³. A demonstrator CTS was designed and implemented in Perl as a CGI program and forms a major part of the output of the SHEBANGS project.

The development of the CTS was constrained by requirements from the user community⁴, the grid infrastructure and the requirements of the relying services (mainly the NGS and portal developers). These requirements are summarised below:

Requirements derived from the user community.

1. End users cannot be expected to possess credentials from which trusted GSI proxy certificates can be derived. Most potential end-users do not possess valid credentials recognised by existing production grids [BRUCE]. Specifically users do not possess digital certificates issued by a trusted certificate authority (see [IGTF]).
2. Grid middleware client tools cannot be assumed to be available to the end-user. Most grid middleware client tools require long and often complex installations. Requiring that the end user install such tools would place a great burden upon the end-user.
3. The end-user will only have access to a Web browser.
4. The end-user will be affiliated to an organisation which provides a Shibboleth IdP.
5. The end user must belong to an organisation or Virtual Organisation (VO) that is recognised by the NGS and whose members inherit a right to use NGS resources.
6. Modifications to the Shibboleth middleware are highly undesirable.

Requirements derived from the relying services, including the NGS:

7. The CTS must use protocols and provide credentials compatible with middleware currently supported, or committed to, by the NGS.
8. Any resulting credentials must be compatible with the NGS Security Policy [NGSSEC].
9. Modifications to service middleware are highly undesirable and should be avoided.
10. Modifications to portals, if required at all, must be minimal.

Requirements derived from compatibility with the current NGS infrastructure:

11. Identity assertions must be consumed as SAML assertions via the Shibboleth Protocols (points 4&5; see also the Background section).
12. Translated assertions must be GSI credentials (points 7&8).
13. A portal must be able to obtain an end-user's delegated credential (points 2,3&8).
14. MyProxy protocols must be used (points 3&13).
15. Authorisation must be achieved via grid-mapfile or VOMS mechanisms (points 7&8).

Requirement (7) implies that the solution must be compatible with Globus Toolkit (GT) version 2 (GT2), or the pre-Web Service components of GT4, or the Virtual Data Toolkit (VDT) distribution of GT. This rules out in the short term any solution that would make the NGS gatekeepers depend on PERMIS or CAS, for which support exists only in the Web

3. Indeed, we developed and tested a test CTS that used LDAP authentication (Shibboleth not yet being available in production) for a portal to a campus grid.

4 The status of the user-community was obtained through liaison with the NGS support team and observed minimal operational software stacks available i.e. access to a Web browser.

Service components of GT4. However, this does not rule out a dependency on EGEE's Virtual Organisation Membership Service (VOMS) which is re-distributed through VDT and already a commitment in the NGS roadmap. Requirement (8) implies that any task executing on NGS resources must be traceable to the initiating end-user. In our solution, this will require that the Shibboleth attribute server be able to provide a Common Name (or pseudonym), unique within the user's home institution; we believe that this is not unreasonable to ask of an organisation wanting to authorise its users to access NGS.

The CTS CGI script and the VOMS::Lite library are described in the next section.

Outputs and Results

How a task is granted the permission to be executed on a given resource is governed by the resources ability to identify the entity wishing to perform the task and the relationship between the identity and its rights to perform the task. This is the conventional view of authentication and authorisation in established grids today. Shibboleth is somewhat more concerned with identity and can only provide further attributes which make sense within the reach of an end-user's administrative domain⁵. In the grid infrastructure that we target with SHEBANGS, authentication and authorisation are handled separately, and we must consider both. It is not enough to assert an end-user's identity to the grid; we must also provide a mechanism that enables the grids to make the subsequent authorisation decision.

We achieved this in the CTS by considering the CTS as a Virtual Organisation (VO) which represents an entire Shibboleth federation (or subset thereof). This has obvious flaws discussed later but it is a necessary step in the description of the evolution of the SHEBANGS project. The following describes the CTS in its first realisation.

Authentication. In this approach, a user accessing the CTS is authenticated by a Shibboleth IdP operated by the organisation with which the user is affiliated. The InQueue federation [INQUEUE] was used to provide the WAYF service (see Figure 1, steps 2-4) and authentication through various IdPs was thus enabled. Furthermore, the IdP of the FAME-Permis [FAME-PERMISS] project was available via InQueue and the CTS evolved to be able to consume Level of Assurance Attributes [NIST-LoA, PERMISS-LoA].

Authorization. In a GT2-based Grid, such as the NGS, the right of a user to access a Grid resource is established by the existence of a mapping from the Distinguished Name (DN) on the user's X.509 certificate to an account (or pool of accounts) on the target resource. As we were avoiding any modifications to existing middleware (see requirements 6,9&10 above), we had to solve two problems:

1. to generate a certificate with an appropriate DN so that the Grid resource can authenticate the user, and
2. to arrange that that the DN is mapped to a (pool) account that the end user is entitled to access, hence enabling the Grid resource to authorise the user.

We solved (1) by introducing the CTS. The CTS uses Shibboleth methods to obtain SAML assertions about the user, and translates these into GSI credentials which it uploads (delegates) to a standard MyProxy server, returning to the user the information (username, password, and URI) necessary either to retrieve a proxy from the MyProxy server directly or to delegate a proxy to a portal. The CTS thus acts as a Shibboleth Service Provider (SP), an online Certificate Authority (CA), a GSI client tool, and a MyProxy client. This process is illustrated in Figure 1.

A solution for (2, the authorisation) is important for usability, for without this, a user would need to negotiate out-of-bands with the grid resource provider for access privileges. Fortunately, this problem — delegating the authorisation decision to a trusted *Virtual Organisation* (VO) — is not new, having been addressed at least partially by *e.g.* CAS,

⁵ Provision of attributes targeted at a specific VO is not scalable, since the number of possible VOs far exceed the number of individuals within any given federation.

VOMS, and PERMIS. For the reasons given above, we partially adopted the VOMS solution, adding VOMS attributes (non-critical X.509 extensions) to the proxy credentials delegated by the CTS. In this way, when making the authorization decision, the grid resource provider can take into account the attributes provided by the user's home institution to the CTS.

The SHEBANGS project has essentially created a mechanism to pass on identity and other general and VO based attributes within one assertion the GSI credential i.e. we have effected the translation between SAML assertions and X.509/GSI credentials with attribute certificate [ACRFC] extensions.

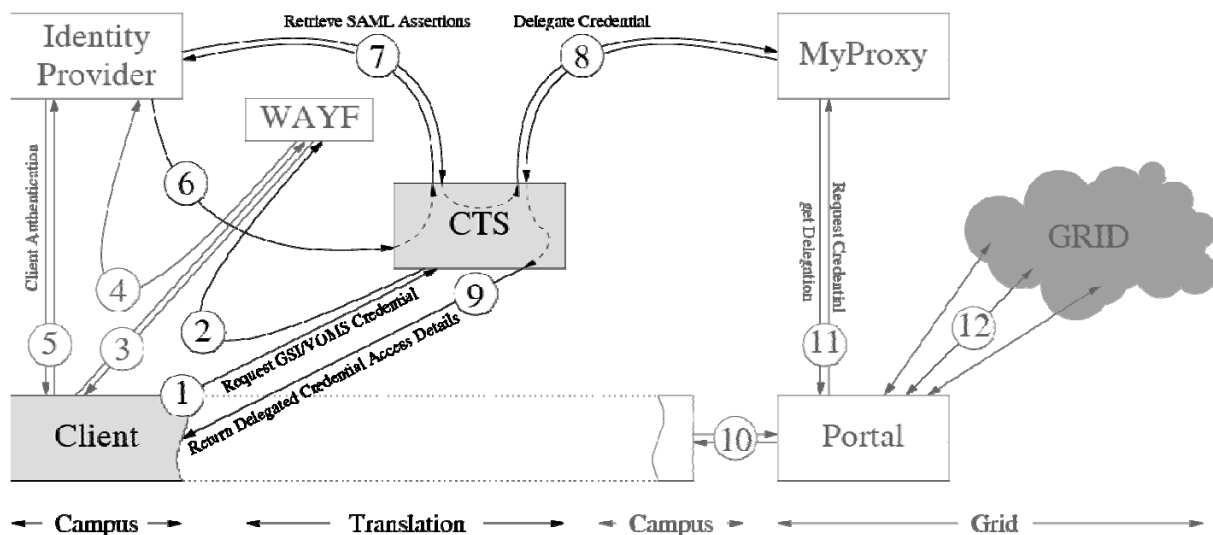


Figure 1: Architecture, showing how a Credential Translation Service can be used to delegate a GSI proxy to a portal, allowing a user, authenticated solely by Shibboleth means, to access the NGS.

1. A user, perhaps referred by an HTML link from the portal, points their browser at the CTS.
2. The user's browser is redirected to a trusted Where Are You From (WAYF) service.
3. The WAYF server presents a form which the client completes and posts back to the server.
4. The user's browser is now redirected to the appropriate institution's IdP.
5. Out of bands authentication takes place between the user and the IdP.
6. The IdP redirects the browser back to the CTS (passing Shibboleth artifacts in the URL).
7. The CTS uses the artifacts to obtain SAML Assertions from the IdP on a secure back channel. The CTS evaluates the SAML Assertions and issues a GSI Credential.
8. The CTS delegates this credential to a MyProxy Server.
9. The CTS returns a web page over HTTPS to the client which contains a MyProxy username:password:server triplet.
- 10-12. The user logs into the portal using the MyProxy triplet, and is now able to use the Grid.

Identity Attributes – the X509 credential

The mapping between SAML attributes and X.509 names (as used in the Distinguished Name (DN) of an X.509 certificate) is not straightforward. SAML provides a number of schemes for identifying individuals, but the grids being addressed by this project do not handle individuals with multiple identities well. A grid will treat an end-user who possesses different names as different individuals. Therefore care must be taken when describing the end-user. Fortunately, the choice of which attributes to provide an end-user is generally set once per individual per IdP-SP relationship; in this case the issue is no worse than that

which exists already within the GSI domain as it stands today⁶. Thus the SAML attributes presented to a particular SP may remain constant for an individual within the administrative domain of their IdP. A bespoke algorithm was therefore established to create a suitable GSI identity as follows.

From the Shibboleth protected Web server the CTS CGI script inherits five pieces of information through environment variables:

- HTTP_SHIB_ATTRIBUTES — the end-user specific XML SAML assertion encoded in base64,
- HTTP_SHIB_IDENTITY_PROVIDER — a string representing the organisation to which the end-user authenticated,
- SERVER_NAME — the server on which the CTS runs,
- SERVER_PORT — the port through which the CTS is accessed,
- a variable which lets the CTS know whether the client accessed the CTS securely.

The Distinguished Name Sequence of the X.509 credential produced is configurable. For the SHEBANGS demonstrator, a CTS was constructed according to the following template:

1. countryName = UK
2. organisation = SHEBANGS
3. organisation = NGS
4. organisation = TestCTS
5. domainComponents constructed from SERVER_NAME above
6. organisationalUnit from HTTP_SHIB_IDENTITY_PROVIDER above
7. commonName from HTTP_SHIB_ATTRIBUTES above

For my identity as asserted by the OpenIdP [OPENIDP] this produces a DN of the following form:

"/C=UK/O=SHEBANGS/O=NGS/O=TestCTS/DC=wallace/DC=mvc/DC=mcc/DC=ac/DC=uk/OU=shib13.openidp.org/CN=nimpo"

The commonName attribute was set according to the ranked element in the list below for which only one entry exists in the SAML assertion:

1. urn:oid:2.5.4.3 (X.500 commonName)
2. urn:mace:dir:attribute-def:eduPersonPrincipalName (OID 1.3.6.1.4.1.5923.1.1.1.6)
3. urn:mace:dir:attribute-def:eduPersonTargetedID (1.3.6.1.4.1.5923.1.1.1.10)
4. ResponseID⁷.

In the case of the first three the DN would be constant between visits. ResponseID is always guaranteed to be there and was used as a fall back. If ResponseID is used however the identity seen by the corresponding grid is transient and lasts only as long as the credential. It is also pseudonymous.

Finally, if the Level of Assurance (LoA) attribute is passed in the SAML assertion (as is done by the FAMP PERMIS IdP, OID 1.2.826.0.1.3344810.1.1.104) this LoA is used to select which CA certificate is used to sign the X509 Credential. This representation of the Level of Assurance allows a relying grid service to make authentication decisions based upon the LoA at the IdP. Alternative methods of representing the LoA were considered:

- The addition of a non-critical extension to the X.509 certificate with the same OID was dismissed due to lack of an X.509 binding for this information;
- Adjusting the validity period allowable for the X.509 credential was dismissed as this was deemed an authorisation decision which the CTS is not designed to make.

The multiple CA option best fits practices adopted by the grid community. The IGTF asserts the how trustworthy each CA is based on audit of its procedures and policies and ranks CAs

6 The issue of an identity being related to an institute as with the UK eScience CA or the ability for an individual to have multiple Distinguished Names has been debated elsewhere (e.g. on the OGF ShibGrid mailing list) and the conflict has not been resolved satisfactorily.

7 ResponseID is not a property of the individual but a property of the assertion carrying the identity. It is always available, but it is never the same twice.

according to a number of profiles. These are the Classic, Short Lived Credential Services (SLCS), Member Integrated X.509 Credential Services (MICS), Experimental and Worthless Profiles. Thus, a high security grid service may only want to trust CAs with a high level of trustworthiness and a low security grid service may want to allow access to people with a reasonably lower level of authentication. This can be achieved by placing the relevant CA certificate in the grid services' trusted CA directories according to the profiles.

Authorisation Attributes – the VOMS credential

The VOMS credential is constructed according to the current VOMS specification [VOMSAC] and tied to the DN as constructed above. The VOMS VO is configurable; for the demonstrator CTS, it was set to "/shebangs.ngs.ac.uk". Roles were obtained from the SAML assertions eduPersonPrimaryAffiliation and eduPersonAffiliation, in that order.

CTS usage from an end-user perspective

There are two different ways an end-user might access the CTS. In the simpler (i.e. for the implementer) approach, as shown in Figure 1, the user first approaches the CTS before accessing any grid portal. Figures 2-6 show the end-user experience of a typical "CTS-first" approach for accessing grid resources. The second approach – the "portal-first approach" – streamlines the end-users' experience by using two re-directions (Figure 7). In the CTS first approach the end-user points their browser at the CTS and is presented with the Shibboleth federation's WAYF page (Figure 2). The end-user then selects their institute from the list and is sent to the corresponding login page corresponding (Figure 3). After identifying themselves to their institute's IdP their browser is immediately redirected back to the CTS which places a fresh GSI-VOMS credential in a MyProxy server and presents details to the end-user via the browser (Figure 4). Using the MyProxy server location, username and password the end-user can then exploit any grid portal which recognises the CTS's CA credentials (Figure 5). The user can then access the grid (Figure 6).

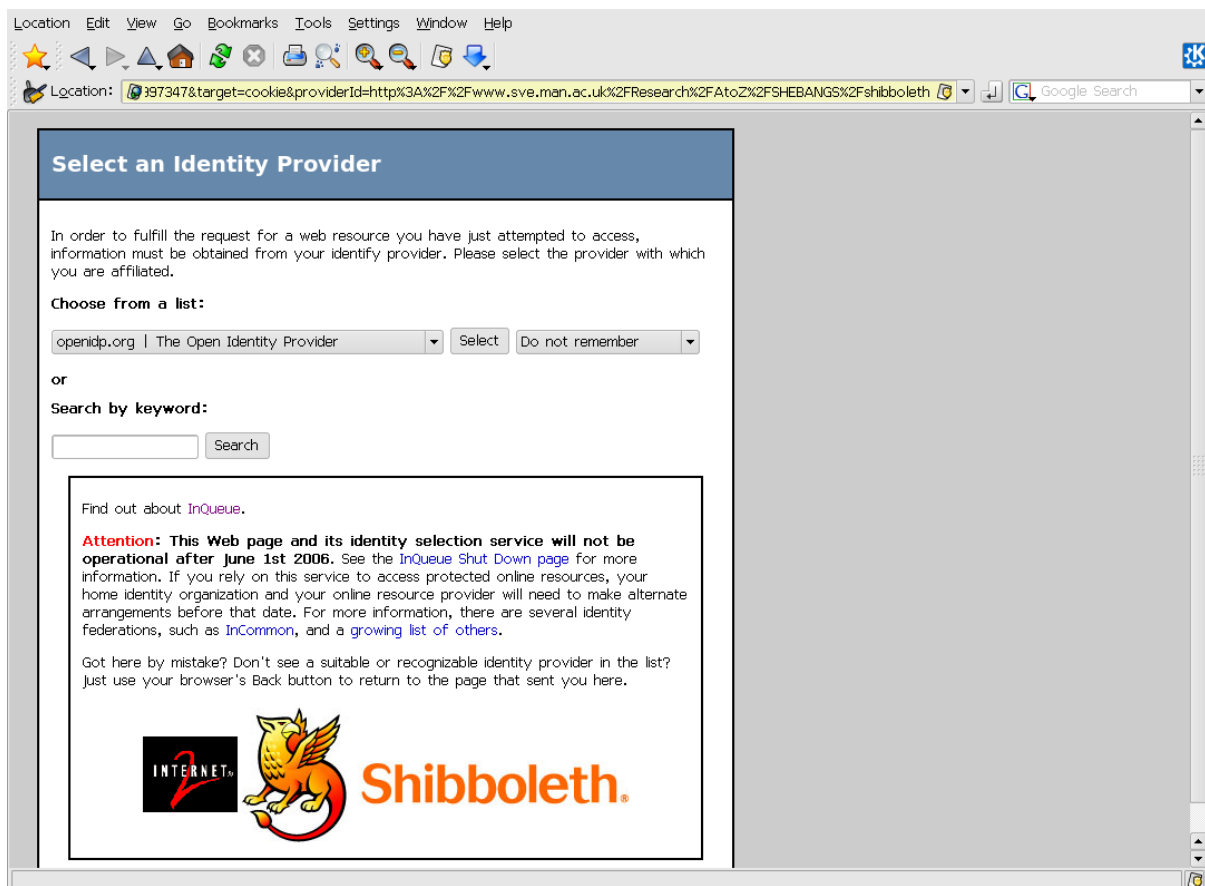


Figure 2 - The CTS redirects the browser to the Shibboleth federation WAYF

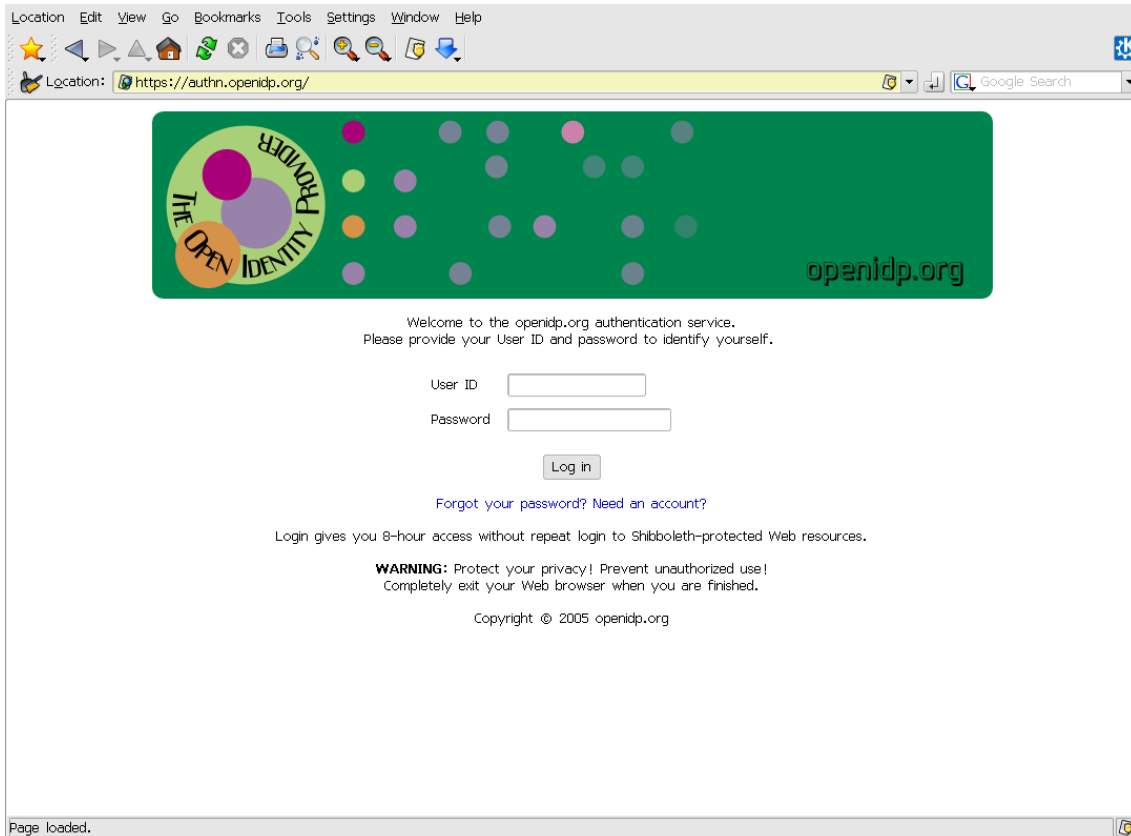


Figure 3 - The end user logs into his or her Identity Provider

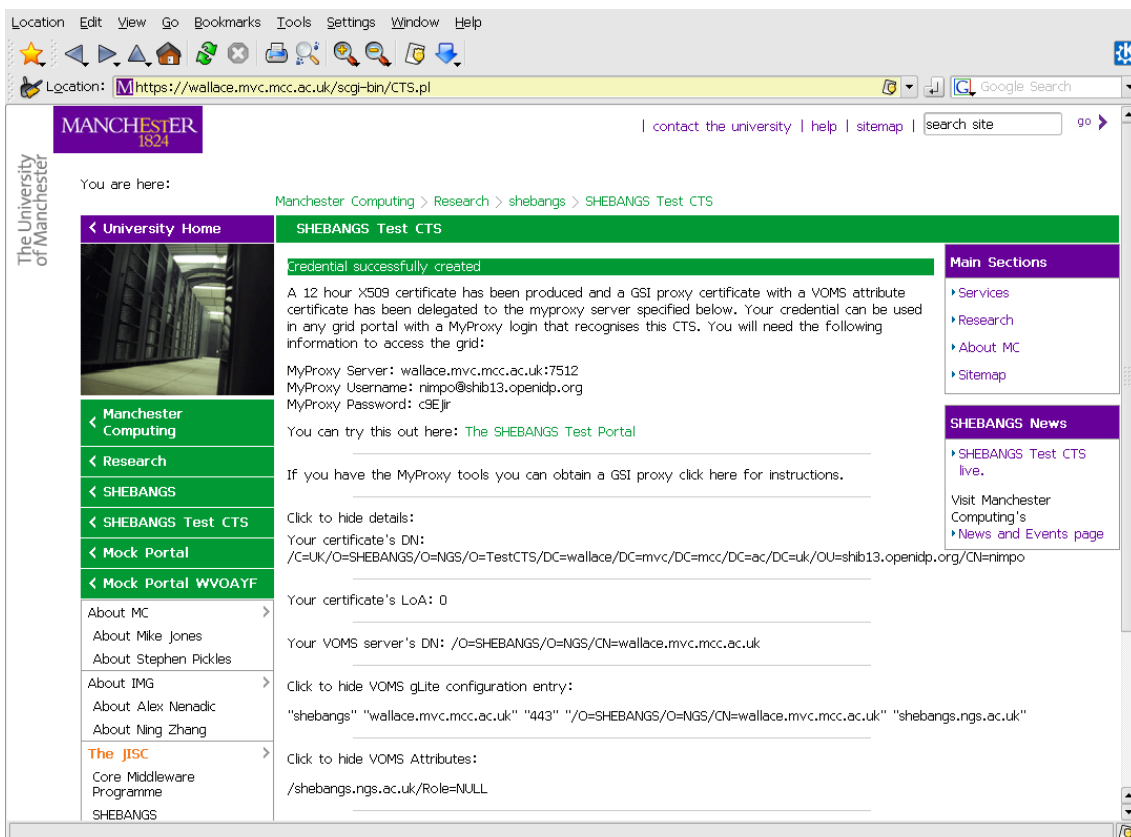


Figure 4 - The browser is re-directed back to the CTS; the CTS creates a Grid credential and places it in a MyProxy server.

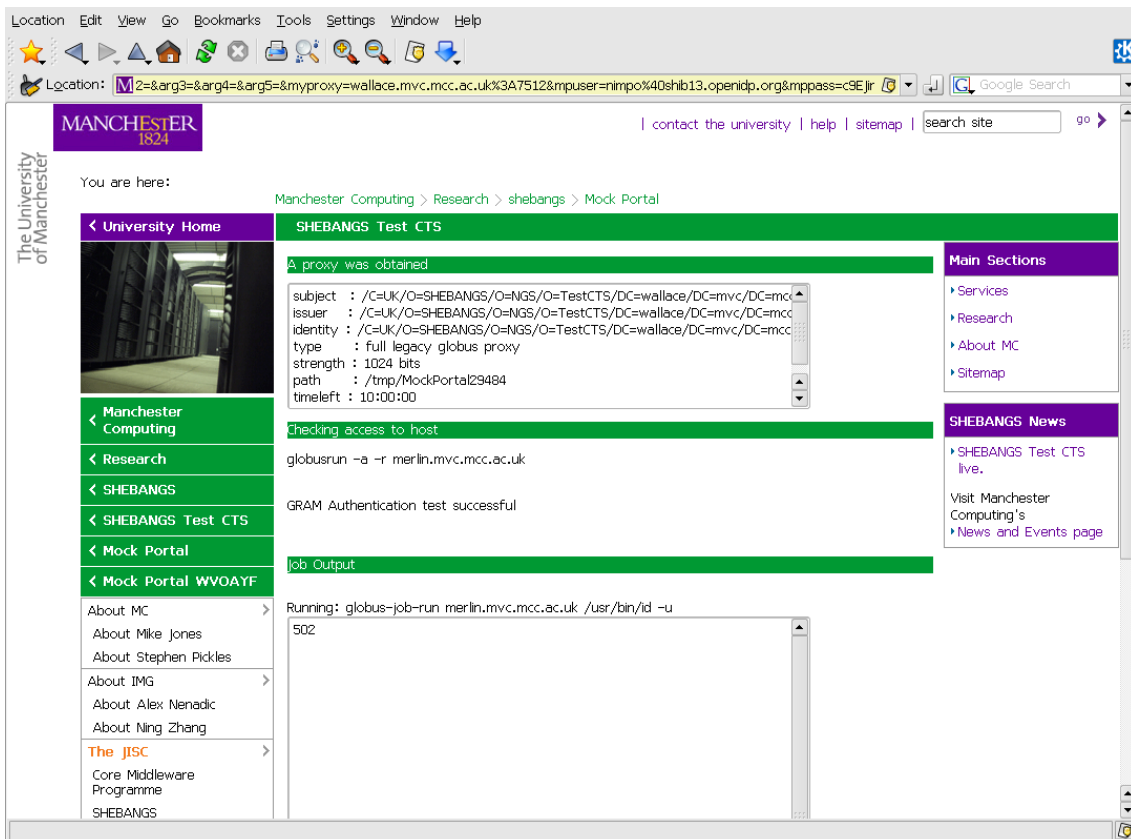


Figure 5 - The end user logs into a portal using his or her new credentials

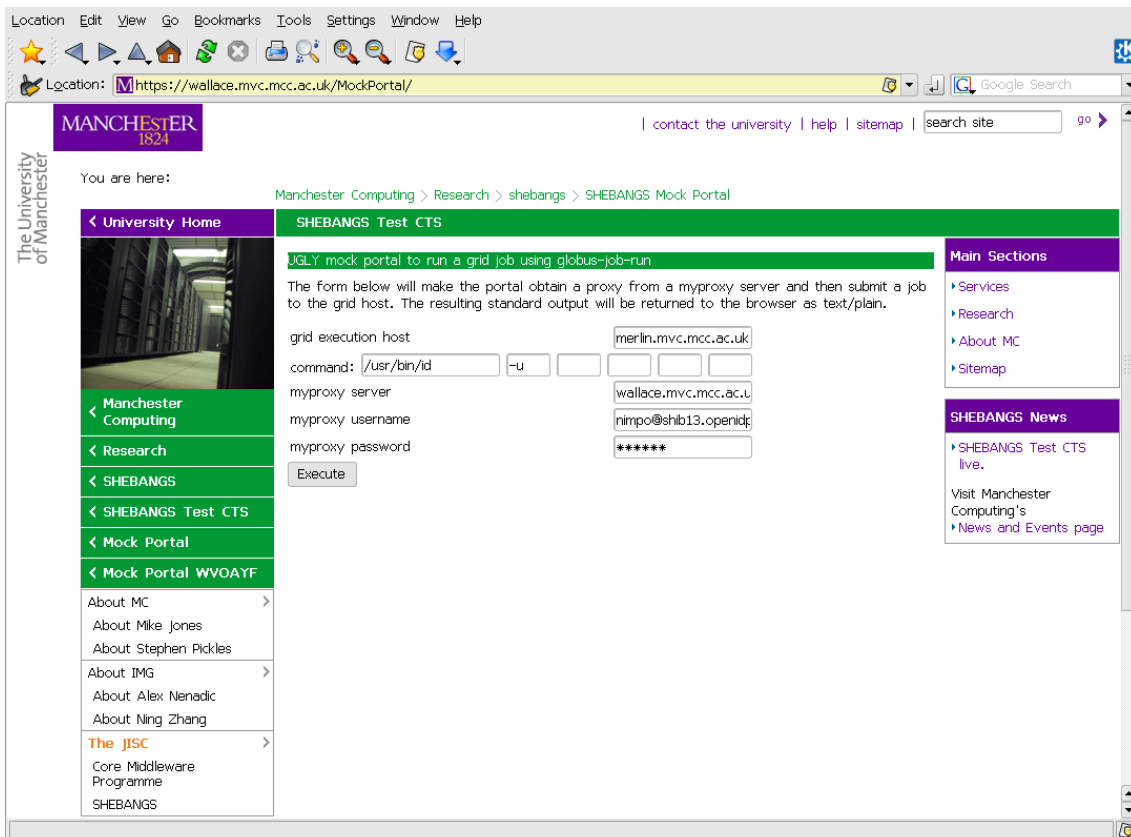


Figure 6 - The portal allows the user to access Grid resources using the new credential.

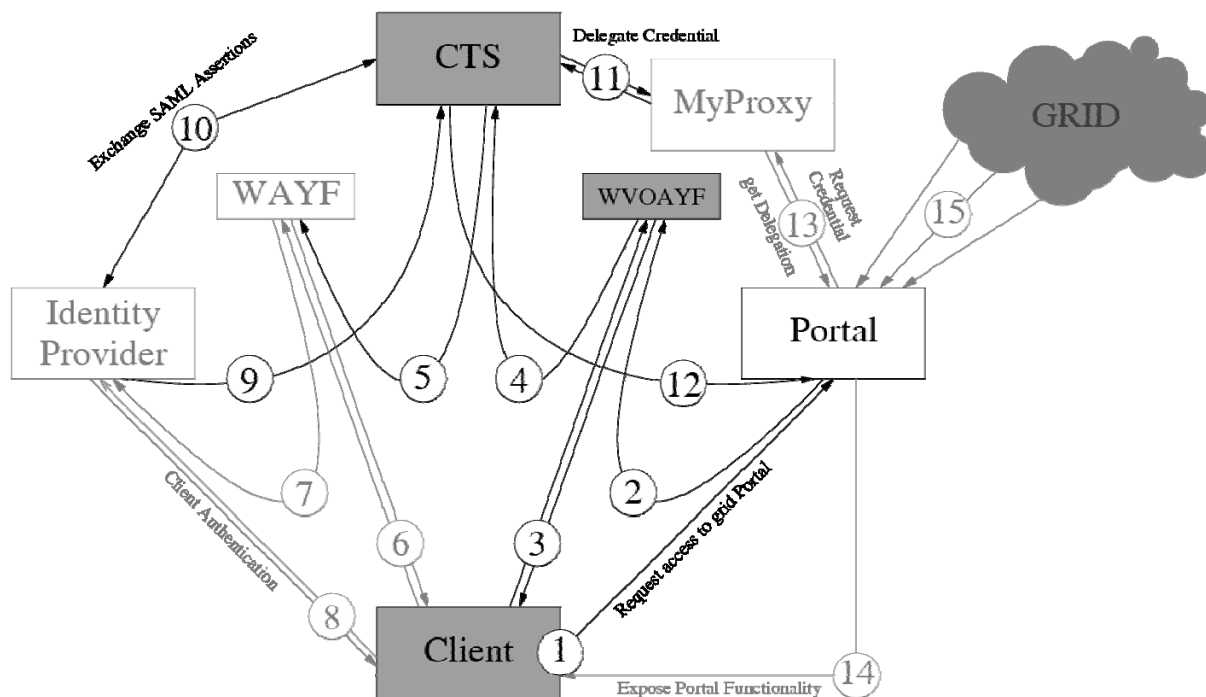


Figure 7 - Architecture of the portal-first approach.

In the portal first approach (Figure 7) the end-user goes directly to the portal to access the grid and is redirected to a WAYF-like service which we dub the “Which VO Are You From” (WVOAYF) service. The end-user never sees the CTS.

Deployment options. The CTS can be deployed independently, permitting clear separation of the roles and responsibilities of operating the Identity Provider, portal, MyProxy server, and Grid resources, and making explicit the trust relationships between these entities. Thus scenarios in which a CTS is run by a university, by the NGS, by another VO, or a combination of these, are all viable. In each case, it is a policy matter for the Grid resource provider to decide which Credential Translation Services it trusts and chooses to support.

Certificate Policy (CP) and Certification Practices Statement (CPS). The CTS, in its rôle as online CA, will be governed by a CPS and will use a subordinate CA certificate signed by an offline CA; if this is the UK e-Science CA, then the CA operator (i.e. the NGS) could effectively revoke all certificates issued by the CTS should this prove necessary. The CTS will typically issue short-lived PKI (X509) credentials, with a lifetime comparable to the 12 hours of a default GSI proxy. The private key need never leave the CTS, as it is only required for long enough to upload a conventional GSI or VOMS proxy to a standard MyProxy server. Where possible, the certificate created in the steps above will have a DN based on the SAML assertions obtained from the IdP. This will allow the CTS to reissue credentials in the same namespace when a requester's identity can be associated with a static identity, which is important if the end-user is to be able to retrieve files from a previous Grid session.

Outcomes

The VOMS::Lite Perl library has been developed. This library was designed to provide all the functionality required for the CTS to operate. It has few external dependencies. Those that it does have are common, well-established Perl libraries of which most are either packaged with standard Perl distributions or can be obtained through CPAN [CPAN]. The library provides subroutines for the creation and examination of GSI, X509 and VOMS credentials according to the current standards available as well as command line tools to exploit these. It contains MyProxy subroutines to delegate proxy certificates to a MyProxy service according to the MyProxy protocol version 2. The library also provides experimental

access to existing VOMS servers using the Perl DBI library interface to MySQL. Documentation for all these library components is available through the normal Perl “Plain Old Documentation” (POD) mechanism.

The CTS implementation is also available and is provided as a drop-in CGI Perl script with documentation and installation instructions. An installation script is provided that creates the necessary CA certificates for a basic service. A demonstrator CTS is currently in place, accessible via link from the SHEBANGS project website, and is open to anyone who is registered with an IdP in the same federation.

The lightweight nature of the CTS which the Virtual Organisations demand is in direct contradiction with the heavyweight trust models which grid environments demand. The work of the ShibGrid Project addresses this very neatly and future work to merge these two projects is vital if any widely deployed solution is to be drawn from this work. As it stands, only a few organisations are in a position to benefit from SHEBANGS on a production scale: those that can invest in a production CA of the scale of the UK eScience CA. This could be alleviated by using certificates generated by FIPS-140 compliant hard tokens, since these would in principle be acceptable by the IGTF; the downside is of course an undesirable proliferation of Certification Authorities.

During the lifetime of the project the UK Federation Shibboleth infrastructure has emerged. Its policies are in stark contrast to those needed for lightweight, dynamic Virtual Organisations to flourish. This federation requires that a legal entity underwrite the service, whereas VOs are by their very nature virtual and consequently it is often difficult to find a legal entity willing to assume legal responsibility for the VO’s actions.

Conclusions

SHEBANGS has proven that using a Credential Translation Service to bridge from the security realm of Shibboleth to that of PKI-based Grids is technically feasible, and it has delivered software to make NGS resources and services accessible to Shibboleth-based portals.

Implications

Limited deployments are likely to occur in the context of normal NGS activities, but the full benefits will not be realized without further work. A holistic rationalisation and integration of the outputs of SHEBANGS and ShibGrid is required to address a broader range of use cases than either can address alone; a preliminary analysis undertaken by SHEBANGS and ShibGrid participants informed the FUSINGS proposal, but this was unsuccessful.

Recommendations

The requirements of Grid computing do not appear to be well represented in the fora where UK access management policy is being made. No doubt the converse is also true. More discussion within and across these communities is needed to establish consensus on the viability of possible deployment scenarios for the SHEBANGS CTS (who hosts it and how is trust established) in the context of the policy of both Identity Management federations (on the Shibboleth side) and Certification Authorities (on the Grid side). For example, the requirement of the UK Access Management Federation for Legal Entities to underwrite Service Providers presents a potential barrier to uptake of SHEBANGS-like approaches. Furthermore, there is a tension between the requirement of Grid computing for strong authentication and that of identity management federations for pseudonymous authentication; it is not clear that attribute release policies developed with the needs of the latter in mind will be entirely satisfactory for the former.

References

- [SHIBGRID] The ShibGrid project web site, <http://www.oerc.ox.ac.uk/activities/projects/index.xml?ID=ShibGrid>.
- [ATHENS] The Athens web site, <http://www.athens.co.uk>
- [NGS STATUS] http://www.grid-support.ac.uk/gosboard/NGS800/National_Grid_Service_Status_Report_December_2006.pdf
- [BRUCE] B. Beckles, P. V. Coveney, P. Y. A. Ryan, A. E. Abdallah, S. M. Pickles, J. M. Brooke, and M. Mc Keown, "A user-friendly approach to computational grid security", *Proceedings of the UK e-Science All Hands Meeting*, 2006.
<http://www.allhands.org.uk/2006/proceedings/papers/636.pdf>
- [IGTF] The International Grid Trust Federation, <http://www.gridpma.org>
- [NGSSEC] The NGS Security Policy, <http://www.ngs.ac.uk/security.html>
- [INQUEUE] The InQueue Federation, <http://www.inqueue.org>
- [FAME-PERMIS] The FAMS PERMIS Project Web site, <http://www.fame-permis.org/>
- [NIST-LoA] W.E. Burr, D.F. Dodson, W.T.Polk, "Electronic Authentication Guideline", NIST Special Publication 800-63 Version 1.0.2, Apr 2006
- [PERMIS-LoA] Aleksandra Nenadic, Ning Zhang, Jay Chin, Carole Goble, "FAME: Adding Multi-Level Authentication to Shibboleth", e-science, p.157, *Second IEEE International Conference on e-Science and Grid Computing (e-Science'06)*, 2006
- [ACRFC] S. Farrell and R. Housley, "An Internet Attribute Certificate Profile for Authorization", IETF RFC 3281, April 2002
- [VOMSAC] Vincenzo Ciaschini, Valerio Venturi, Andrea Ceccanti, "The VOMS Attribute Certificate Format", Draft, OGSA Authorization working group, OGF GWD-I (proposed), 11 Sep 2006
- [CPAN] The Comprehensive Perl Archive Network <http://www.cpan.org>
- [MyProxy] J. Novotny, S. Tuecke, and V. Welch, "An Online Credential Repository for the Grid: MyProxy", *Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10)*, IEEE Press, August 2001, pages 104-111.
- [AHM07] M.A.S. Jones, S.M. Pickles, A. Nenadic, N. Zhang, "SHEBANGS: Shibboleth Enabled Bridge to Access the National Grid Service", *Proceedings of the UK e-Science All Hands Meeting 2007* (accepted).