

e-Infrastructure Proposal Cover Sheet

Cover Sheet for Proposals (All sections must be completed)	<i>JISC Capital Programme</i>
--	-------------------------------

Name of Capital Programme: e-Infrastructure

Programme Strand:
 (Please tick ONE BOX ONLY, as appropriate)

e-Research Community Engagement & Support

<input type="checkbox"/> Call I – Barriers to Take-Up of e-Infrastructure Services	<input type="checkbox"/> Call II – Support for Research: Tools & Standards	<input type="checkbox"/> Call III – Use Cases and Service Usage Models
---	---	---

e-Infrastructure Security	Knowledge Organisation and Semantic Services
----------------------------------	---

Call IV – Federated Tools and Services <input type="checkbox"/> a) Integration of Grid and Shibboleth <input type="checkbox"/> b) Developing and Applying n-tier Web Service Architectures <input type="checkbox"/> c) Applying existing virtual home for identity solutions	Call V – Virtual Organisation Management Tools and Services <input type="checkbox"/> a) Tools for the establishment of VOs <input checked="" type="checkbox"/> b) Services and UIs for management of VOs <input type="checkbox"/> c) Federation membership models for VOs <input type="checkbox"/> d) Delegated authorisation	Call VI – Sematically Coordinating Resources and Services Across Registries <input type="checkbox"/> a) Area A – integration of Resources and Services from Existing JISC Services <input type="checkbox"/> b) Area B – Metadata for Services, Data, and Published Literature
--	--	--

Name of Lead Institution: University of Kent

Name of Proposed Project: Integrating VOMS and PERMIS for Superior Secure Grid Management (VPMan)

Name(s) of Project Partner(s): National E-Science Centre at the University of Glasgow, National Grid Service

Full Contact Details for Primary Contact:
Name: David Chadwick
Position: Professor of Information Systems Security
Email: d.w.chadwick@kent.ac.uk
Address: Computing Laboratory, University of Kent, Canterbury, CT2 7NF
Tel: 01227 823221
Fax: 01227 762 811

Length of Project: 17 Months

Project Start Date: 1 March 2007 **Project End Date:** 31 July 2008

Total Funding Requested from JISC: £145,599

Funding Broken Down over Financial Years (April - March):		
Apr06 – Mar07	Apr07 – Mar08	Apr08 – Mar09
£10,728	£111,845	£23,026
Total Institutional Contributions:		£79,446
Percentage Contributions over the Life of the Project:	JISC 65%	PARTNERS 35%
Outline Project Description		
<p>Both VOMS [1] and PERMIS [2] provide security management infrastructures for Grids but are predominantly used by different groups of Grid users. Each has its strengths and weaknesses and their combination would be a powerful solution to Grid security management as described below. Currently however they are not integrated and the benefits of a combined system cannot be enjoyed. This project proposes to address this directly. Specifically the objectives of this project are to:</p> <ul style="list-style-type: none"> • integrate VOMS and PERMIS, more specifically the VOMS user management and attribute assignment function with the PERMIS policy based authorisation decision function; • ensure they seamlessly inter-work with latest Grid technologies including Globus toolkit version 4 (GT4), the Open Middleware Infrastructure Institute UK (OMII-UK) software release and Shibboleth; • validate the results in several representative major pilot applications run by the National e-Science Centre (NeSC) at the University of Glasgow; • evaluate the combined software from user, administrator and Grid developer perspectives; • integrate the combined infrastructure with the National Grid Service (NGS) at CCLRC; • distribute the integrated software as open source code as part of either Globus Toolkit, or the OMII-UK Repository, or the US-NMI, or a combination of them. 		
I have looked at the example FOI form at Appendix A and included an FOI form in the attached bid (Tick Box)	YES ✓	NO
I have read the Circular and associated Terms and Conditions of Grant at Appendix B (Tick Box)	YES ✓	NO

Integrating VOMS and PERMIS for Superior Secure Grid Management (VPMan)

1. Background

1.1 Managing grids from a security perspective comprises two main functions: the privilege assignment function in which users are assigned to roles, and the authorisation decision function in which policies are set for which roles should have access to which grid resources. These functions typically take place in different systems at different locations. These functions are carried out by the Identity Provider (IdP) and Service Provider (SP) in Shibboleth terminology, and by the VO Manager and grid service provider in grid terminology. More generally, privileges are assigned to users as a mixture of attributes and roles, by one or more attribute authorities (AAs). Attributes (such as login id and department) are assigned by a user's home institution; virtual organisation (VO) roles are assigned by a VO management authority, and professional memberships by learned societies such as IEEE and ACM. These attributes are then transferred to the grid SP, where the authorisation decision function is carried out based on the policy set by the resource's owner. If a user's grid job is accessing multiple resources at multiple sites, then the authorisation decision function may take place several times at several different resource sites using different policies in each case. The Virtual Organisation Management Service (VOMS) [1] provides a well utilised privilege assignment function which is carried out by the VO manager. It is the chosen VO management function of Grid projects such as EGEE, and it is planned to integrate it into the National Grid Service (NGS) at CCLRC. However, its authorisation decision function is intentionally missing by design (it relies on LCAS, see later). PERMIS on the other hand provides a feature rich, modular authorisation decision function, with a user friendly policy management interface, is already integrated into Shibboleth and is currently being integrated into the OMII-UK software environment by the London E-Science Centre (LESC). However, it has a less well developed privilege assignment function. This project proposes to integrate the privilege assignment function of VOMS with the authorisation decision function of PERMIS, so that the management of grids becomes easier, whilst simultaneously allowing finer grained more feature rich authorisation infrastructures to be designed and built. We expect the combination of these technologies to have a significant impact across the UK and international e-Science communities.

1.2 In the above discussion we note that several other features were mentioned, namely: the ability to use attributes assigned by multiple AAs for authorisation decisions, and the ability to run grid jobs at multiple sites. These particular issues are being addressed in companion proposals, namely Shintau and nDoA respectively, and if funded, their results will be compatible with those of this proposal.

2. Background to VOMS

2.1 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*" [6]. Even though it is only a simple account database, nevertheless the account management is well developed and has the concepts of *groups, subgroups, roles* and *capabilities*. *Groups* may contain *subgroups* nested to any depth, with the most superior group being the VO. A member of any subgroup is also a member of all the superior encapsulating groups up to that of the VO. *Roles* and *capabilities* are assigned to VO members within a group context. *Roles* signify the roles a user has within a group context, and *capabilities* signify permissions to perform certain tasks within a group context (although it is understood that capabilities are currently being withdrawn). When a user runs a grid job, all their group memberships are automatically included in their credentials that accompany the request, but the user can choose which roles to include in these credentials. Roles and capabilities are encoded as free format strings, and so in principle can contain anything that the authorization decision function will understand.

2.2 The user credentials are actually encoded as X.509 attribute certificates [7] containing fully qualified attribute names (FQAN) in the following format:

/VO[/group[/subgroup(s)]]/Role=role[/Capability=cap]

2.3 VOMS is integrated with the Globus Toolkit so that the user's credentials can be passed around with the grid job, embedded inside the user's proxy certificate. A modified version of Globus *grid-proxy-init* produces a proxy certificate that includes the user's VOMS credentials. VOMS supports multiple VO authorities allowing users to include multiple attribute certificates from multiple VOMS servers in their proxy certificates, providing a user has the same distinguished name at each server.

2.4 Authorisation decision making in VOMS is carried out by LCAS [8]. LCAS is a shared library integrated into the Globus Toolkit, and called when an authorization decision is needed. LCAS provides three default authorization modules:

- `lcas_userallow.mod` - that checks the grid map-file to see if the user is allowed access
- `lcas_userban.mod` - a blacklist that checks if the user should be banned from access
- `lcas_timeslots.mod` - that checks if the resource is available at that time.

An additional optional plugin `lcas_voms.mod` decides if the user is authorized based on the VOMS credentials stored in the user's proxy X509 certificate. As one can see, this authorization decision function is not very sophisticated or scalable since it relies on lists of usernames and cannot be used to construct fine grained policies. To quote the authors of VOMS: "*In the authors' opinion, PERMIS is clearly superior to VOMS as a policy engine*" [1].

2.5 VOMS is attempting to rectify some of its deficiencies with the G-PBOX work [18], which is producing a set of tools for policy management that will allow XACML policies and VOMS attributes to be used for authorising Grid jobs. The interface between the Grid application and the XACML PDP is an XACML request/response context, but it is not known at this time what protocol will be used to carry the XACML contexts. In parallel with (but separate from) the G-PBOX work, the OGF OGSA-AuthZ group, chaired by the PI of this proposal, is defining an XACML profile to be used for carrying the XACML request/response context between a PEP and a PDP for grids [25]. PERMIS is migrating to this protocol. The VOMS architects have been invited to join in this work so that a common standard for this interaction can be defined. It is proposed to use this OGF profile in this proposal.

3. Background to PERMIS

3.1 The main strength of PERMIS, and the primary focus in its development, has been its modular construction [16] and compliance with standards. It supports X.509 attribute certificates [7], policies in XML, Shibboleth attribute assertions, the OGSA Authz protocol [3] and LDAP repositories. It is currently being migrated to the OGSA XACML Authz protocol [25]. PERMIS comprises two components: a credential validation service (CVS), and a policy decision point (PDP). Both components are policy driven. CVS policies are of the form "this authority is trusted to assign these attributes to this group of users, and delegation to depth n is or is not allowed". PDP policies are of the form "users with this set of attributes are allowed this type of access to this resource, providing that the following conditions are met". The PERMIS PDP provides similar functionality to the XACML PDP (although both have features the other does not support). XACML has no equivalent functionality to the CVS [20]. Some of the more notable features of PERMIS include:

- authorisation policies can be created via a user friendly GUI [9] and a new Policy Wizard;
- arbitrary conditions can be set on parameters such as the time of day and the user's request e.g. only grant access if requested memory is less than 30 GB or the local time is after 8pm;
- users may be allowed to dynamically delegate their privilege attributes to other users for a specific period of time e.g. a researcher may delegate the "guest of project X" attribute to a colleague to allow the latter to run a series of experiments for one week. Note that neither SAML [4] nor XACML[5] are able to support this feature since issuers and subjects are specified differently, hence chaining credentials together cannot be supported;
- it supports history based separation of duties, i.e. is stateful, so that users can be forbidden from performing multiple tasks or holding conflicting roles that would allow mistakes or fraud to occur, e.g. it can require that two different scientists validate a set of results before they are released to the public domain. The publicly available XACML PDP cannot do this as it is a stateless PDP.

3.2 The PERMIS architecture is modular, very flexible and scalable and different components of PERMIS can be plugged into different architectures. This has already been shown in previous

projects, for example:

- Grid API - which integrated PERMIS with GT3 and GT4 [19],
- SIPS - which integrated PERMIS with Shibboleth and Apache [21],
- GridShibPERMIS - which integrated PERMIS with GridShib [10],
- A project at CCLRC which has integrated PERMIS with .NET and Python [23]
- A project at LESC which is integrating PERMIS with the OMII-UK software environment.

3.3 PERMIS has concentrated much less on the way that attributes are assigned to users. Indeed the PERMIS decision engine does not care how this is done, and assumes it can be done in many different ways. Consequently, PERMIS supports a set of policy rules (in the CVS) to constrain which attribute assignments are trusted/allowed to take place. PERMIS can let other software assign attributes, for example, organisations may assign attributes to users using SIGNET and GROUPER [22], as is supported in the PERMIS-Shibboleth integration. PERMIS also provides its own tools to make attribute assignments (as digitally signed X.509 attribute certificates (ACs)) and these are stored in LDAP directories. The Delegation Issuing Service of PERMIS [11] uses these digitally signed ACs to allow users to dynamically assign (a subset of their) attributes to other users. VOMS on the other hand allocates unsigned plain attributes to users and stores these in its VOMS database. VOMS requires the VO Manager to delegate attributes to users. ACs, signed by the VOMS server, are then created on demand when a user initiates a grid job. In all cases the PERMIS CVS uses its policy rules to validate the attribute assignments, regardless of which software produced them.

4. Project Proposal

4.1 GT4 and OMII-UK represent two of the most predominant Grid middleware used throughout the UK. As such any unified authorization infrastructure needs to be harmonized with them. To achieve this we propose several case studies that will demonstrate how VOMS and PERMIS can be integrated and applied across a range of e-Science projects building on GT4 and OMII-UK software. We will also show how these technologies can be applied to support Shibboleth based access to a variety of services where fine grained PERMIS authorization utilizing VOMS attributes is needed.

4.2 The first integration will use GT4 as the grid transport mechanism and Policy Enforcement Point (PEP), using the existing modified *grid-proxy-init* to pick up VOMS assigned ACs, and the existing PERMIS CVS and PDP will validate the credentials and make authorization decisions. The second integration scenario will use OMII UK's WS-Security based security infrastructure to transfer a user's VOMS credentials from the VOMS server to the Grid Service Provider, and the PERMIS CVS and PDP will validate the credentials and make authorization decisions at the SP site. The third scenario will use Shibboleth for user single sign on to initiate the transfer of the VOMS attributes needed to make authorization decisions at the PERMIS CVS and PDP. To support these scenarios in a realistic large scale setting, we plan to exploit several major e-Science projects at the NeSC.

5. Project Objectives

5.1 The project objectives are to:

- integrate VOMS and PERMIS, more specifically the VOMS user management and attribute assignment function with the PERMIS policy based authorisation decision function;
- ensure they seamlessly inter-work with the latest Grid technologies including Globus Toolkit version 4 (GT4), the Open Middleware Infrastructure Institute UK (OMII-UK) and Shibboleth;
- validate the results in several representative major pilot applications run by the NeSC;
- evaluate the combined software from user, administrator and Grid developer perspectives;
- integrate the combined infrastructure with the National Grid Service (NGS) at CCLRC;
- distribute the integrated software as open source code as part of either Globus Toolkit, the OMII-UK repository, or the US-NMI, or a combination of them.

6. Pilot Demonstrator with GT4

6.1 The MRC funded Virtual Organisations for Trials and Epidemiological Studies (VOTES) project

(www.nesc.ac.uk/hub/projects/votes) is a 3 year project looking at building a Grid framework for clinical trials and observational studies. The project began in October 2005 and involves NeSC and partners at Oxford, Nottingham, Leicester and Imperial College. A key aspect of the work is that VOTES is not concerned with developing a single Grid infrastructure for a specific clinical trial or study, but with developing a Grid based framework through which a multitude of clinical trials can be supported. The VOTES project has already developed initial prototypes proving proof of concept based upon existing clinical data sets and software resources used across Scotland [12-15]. Versions of this framework utilize GT4, OGSA-DAI, GridSphere and PERMIS.

6.2 Clinical trials and clinical systems place many demands upon security infrastructures to support the various activities that are involved. In particular, the typical processes involved in a clinical trial will comprise recruitment, collection of data specific to the trial and overall management of the trial itself, e.g. to ensure that it is undertaken according to ethical concerns. Fine grained security is essential in this context to ensure that the right data is made available to the right people for the right purpose.

6.3 In this demonstrator we will show how VOMS can be used to manage user attributes specific to the clinical trials VOs, and can be delivered by GT4 to PERMIS to enforce policy decisions on data access and usage. This service will be tested by the clinical trials researchers at the University of Glasgow and across the VOTES partners. Evaluation of the overall management effort required to support this infrastructure will be documented in detail.

7. Pilot Demonstrator with OMII-UK

7.1 The EPSRC pilot project *Meeting the Design Challenges of nanoCMOS Electronics* (nanoCMOS) (www.nesc.ac.uk/hub/projects/nanocmos) started in October 2006 [19]. This project is lead by the University of Glasgow with the e-Science component lead by NeSC Glasgow. The electronics domain demands infrastructures that support protection of intellectual property, be it for designs of transistors, data sets, simulation codes. The quantum level effects of devices of ever decreasing dimensions are becoming ever more important and atomistic simulation of devices is necessary. The nanoCMOS project plans to develop an infrastructure through which device level designs and simulations can be linked through to higher level circuit and system simulations, to predict the overall behavior of complex electronics systems. This will require both large scale HPC usage including access to and use of the NGS, and will generate many terabytes of data. It is planned that the project will exploit OMII-UK middleware to Grid enable simulations; use the OGSA-DAI components of OMII-UK for data access and integration; use the myGrid components of OMII-UK to define and enactment workflows. In all cases requirements and feedback for extensions to these software components will be provided to OMII-UK development teams to ensure that the software meets the requirements/expectations of the nanoCMOS developers and electronic design communities.

7.2 In this application, we will show how VOMS can be used to manage the attributes specific to the teams involved in nanoCMOS design and how PERMIS integrated into the OMII-UK software environment can be used to enforce security policies based on these attributes. These policies will control access to: OMII-UK based GridSAM services accessing the NGS compute nodes; electronic data sets hosted by NGS data nodes; and resources on other HPC nodes across partner sites.

7.3 The integration will be based on the upcoming release of OMII-UK software containing the integration of PERMIS, and the planned SAML interface to the VOMS server. (Currently VOMS uses a proprietary protocol for accessing the VOMS server, but the SAML interface is scheduled for first prototype release in April 2007.) In this demonstrator we will use open web services protocol specifications throughout. We propose to validate the integration of PERMIS and VOMS, the migration of VOMS from its proprietary protocol to a standards based one, and the migration of OMII-UK and PERMIS from the 1st generation [3] to 2nd generation [24, 25] OGSA AuthZ protocols. The requirement to migrate OMII-UK from the 1st generation protocol based on SAMLv1.1, to the 2nd generation protocol based on XACML has already been fed into the OMII-UK User's Forum through Prof Sinnott who is a member. NeSC were one of the early adopters of the 1st generation protocol and were the first to point out its limitations with regard to its inability to pass action parameters to the PDP).

8. Pilot Demonstrator Utilizing Shibboleth, OMII-UK, GT4 and GT2

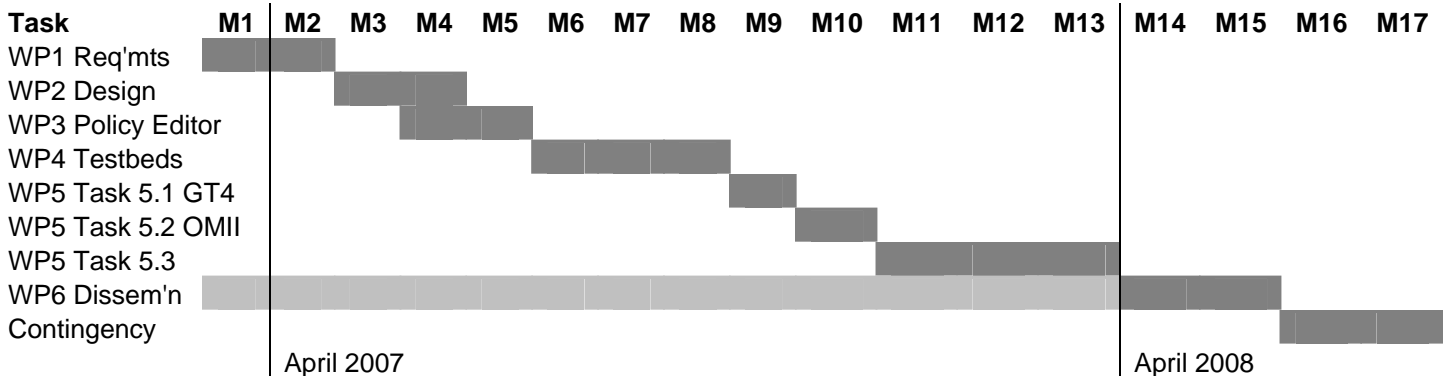
8.1 This demonstrator is the most challenging. Given the different protocol possibilities for initiating grid services, it is important to show how these can all be integrated together effectively. This pilot will allow us to access combinations of GT4/OMII-UK services through Shibboleth single sign on. The scenario envisages a GT4 BLAST service using the NGS for data analysis, combined with an OMII-UK OGSA-DAI data service on the NGS which provides access to nucleotide or protein sequences. A user, who has a globally unique name, will gain access to the NGS OGSA-DAI data, which is protected by PERMIS, by providing a combination of attributes from his Shibboleth IdP and his VOMS server. Once the user is authorized, the data will be obtained and the user will then invoke the GT4 BLAST service on the NGS which requires further IdP and VOMS attributes in order to be authorized by PERMIS. In this scenario we are not promoting a GT4 vs OMII-UK competition, but rather we are showing how we can still have cross-Grid middleware security based on attribute based authorization when both GT4 and OMII-UK are used by different grid service providers.

8.2 Furthermore we recognize that the NGS currently supports earlier versions of Globus (GT2) and different mechanisms for GT2-based job submission to the NGS clusters, e.g. through portals such as portal.ngs.ac.uk. We will demonstrate how a Shibboleth protected version of this portal (or a similar portal since this portal is to be redesigned in the near future) can have different virtual organization policies and attributes associated with it based on PERMIS and VOMS respectively. These include VOs that are allowed to submit jobs to a given NGS cluster only, to the NGS compute clusters or to the data clusters only, or to all the NGS clusters. Extensions to these scenarios include controlling access to specific partner/affiliate sites (rather than the core nodes) or potentially commercial sites. These different scenarios may well provide a rich vein of authorization requirements and challenges, including supporting models of accounting which in the post-fEC era are essential.

8.3 This case study will allow NGS and affiliate sites to better understand and subsequently decide how their resources can be made available and the practical ramifications thereof. Thus partner sites may want to define, monitor and authorize the amount of access on a VO-specific level as well as that described in their NGS service level description. Such information will also be needed for future resource broking and job schedulers to be rolled out across the NGS.

9. Work Packages

VPMan Gantt Chart



WP1. Requirements and information gathering

Understand the precise semantics and current usage of groups, subgroups, roles and capabilities within VOMS applications. Find out how they are being used today for authorization decision making. Understand the relationship between the 3 default LCAS modes and the VOMS mode. Understand how this integrates into Globus Toolkit and can be integrated into OMII-UK, and its relationship with other access control mechanisms such as LCMAPS and GACLs. Production of detailed requirements for case studies utilizing VOMS, PERMIS and Shibboleth with GT4 and OMII-UK, and for GT2

based job submission systems such as Grid portals. Liaise with other on-going JISC funded projects in this area (e.g. ShibGrid and SHEBANGS) as well as utilizing the knowledge of the project partners.

Effort: 1.5 m months (Kent) 0.5 m months (Glasgow) 1 m week (NGS) 1 m week (OMII)

Deliverables

D1.1 A document describing the background to the integration work.

D1.2 A document of case studies to be supported

WP 2. VOMS-PERMIS Integration Design

Describe how VOMS and PERMIS will be integrated into GT4 and OMII-UK, and how the other SP components (LCAS, LCMAPS etc.) will be utilized (or not). Give the first draft to the Globus team in the USA, the OMII-UK team responsible for the OMII-UK security roadmap, and the EGEE VOMS team in Italy. Revise according to their comments and feedback. (Please note that time has been included in the Gantt chart for this.) Interface with OMII-UK to ensure that necessary APIs are defined in their roadmap and implemented to support our integration efforts.

Effort: 1.5 m months (Kent), 0.5 m months (Glasgow), 1 m week (NGS) 1 m week (OMII)

Deliverables

D2.1 A VOMS-PERMIS integration design document.

WP3. Modify the PERMIS Policy Editor and Wizard

Modify the PERMIS Policy Editor and Policy Wizard so that it will be easy to create policies that specify permissions based on VOMS groups, subgroups and roles.

Effort: 1.5 man months (Kent)

Deliverables

D3.1 A modified PERMIS Policy Editor and Wizard with documentation and help files

WP4. VOMS-PERMIS and Shibboleth Integration and Test-bed establishment

Install and configure VOMS. Integrate VOMS and PERMIS into GT4 and OMII according to the design produced in WP2. Build a VOMS PIP for extracting VOMS groups and roles. Build a distributed grid test bed across both sites and test and debug the integration. Prepare the infrastructure for the case studies including policy specification, Grid services, portal and portlet developments and establishment of Shibboleth IdP and SP including ensuring services run on the NGS and can access data hosted on the NGS. Look towards the Shibboleth enabling of the NGS portal and its enhancement and incorporating VOMS-PERMIS authorization scenarios. If needed adapt existing GridSphere portal solutions utilizing the Java-CoG toolkit for GT2 based job submission developed at NeSC as part of the JISC funded GLASS project.

Effort: 3 m months (Kent), 2 m months (Glasgow), 1 m week (NGS) 1 m week (OMII)

Deliverables

D4.1 Beta software ready for validation and piloting.

D4.2 Preparation of test bed, services and portals

WP5. Run the Demonstrators to validate the Integration in e-Science applications

Task 5.1 GT4 Demonstrator of VOMS-PERMIS

Task 5.2 OMII Demonstrator of VOMS PERMIS

Task 5.3 Combined demonstrator of VOMS-PERMIS, Shibboleth, GT2, GT4 and OMII-UK

Effort: 3 m months (Kent), 5 m months (Glasgow), 1 m month NGS 1 m month (OMII)

Deliverables

The primary outputs from WP5 will be in the form of dissemination and include:

D5.1 A paper for an international grid conference describing the piloting of the integrated VOMS-PERMIS software with GT4 and/or OMII-UK.

D5.2 A paper for an international grid conference describing the piloting of the integrated authorization software utilizing Shibboleth and multiple Grid middleware (GT4 and OMII-UK) including how user single sign-on across a range of UK e-Science resources can be supported with fine grained authorisation.

D5.3 Document describing the overall lessons learned in supporting this infrastructure from a user, an administrator and a Grid developer perspective (this includes managers of the NGS and VO administrators wishing to utilize resources such as the NGS and end users of the NGS)

WP6. Dissemination

Build a project portal at the beginning of the project and add this to the PERMIS, NeSC and NGS web sites. Integrate the validated software into the NGS. Package the software along with Globus Toolkit, OMII-UK and/or NMI. Produce user friendly documentation, installation guides and tools.

Effort: 3 m months (Kent), 1 m month (Glasgow), 1 m month (NGS) 1 m month (OMII)

Deliverables

D6.1 The integrated software packaged with GT4 and OMII-UK and fully integrated into the NGS

D6.2. User, developer and administrator documentation for the integrated VOMS-PERMIS package including support in a Shibboleth-enabled environment, with guidance to Grid Operations Support Centre on practicalities of usage

D6.3 Final report to JISC

10. Budget and Value for Money

	March 07	Apr 07– Mar 08	Apr 08– Mar 09	TOTAL £
Directly Incurred Staff at Kent				
RA 13.5 months 100% full time	£3,231	£39,552	£1,552	£44,336
Non-Staff at Kent				
Travel and expenses	£250	£1,750	£2,000	£4,000
Hardware/software	£0	£1,500	£0	£1,500
Other	£100	£1,000	£300	£1,400
Total Non-Staff (B)	£350	£4,250	£2,300	£6,900
Directly Incurred Total (A+B=C)	£3,581	£43,802	£3,852	£51,235
Directly Allocated				
██████████	████	██████	████	████
██████	████	██████	████	████
Directly Allocated Total (D)	£1,334	£16,210	£4,052	£21,596
Indirect Costs (E)	£2,426	£29,108	£2,304	£33,838
Total Project Cost Kent	£7,341	£89,120	£10,208	£106,669
Directly Incurred Staff at NESC				
RA 9 months 80% full time	£1,325	£16,368	£5,680	£23,373
Non-Staff at NESC				
Travel and expenses	£250	£1,750	£2,000	£4,000
Hardware/software	£1500			£1,500
Other	£400	£1,200	£400	£2,000
Total Non-Staff (B)	£2,150	£2,950	£2,400	£7,500
Directly Incurred Total (A+B=C)	£3,475	£19,318	£8,080	£30,873
Directly Allocated				
██████████	████	██████	████	████
██████	████	██████	████	████
Directly Allocated Total (D)	£839	£10,307	£3,474	£14,620
Indirect Costs (E)	£1,755	£21,061	£7,020	£29,837
Total Project Cost NESC	£6,069	£50,686	£18,574	£75,330
Directly Incurred Staff at NGS and OMII				
RA 2.75 months @ £38Kpa NGS		£5,554	£3,173	£8,727
RA 2.75 months OMII		£4,989	£2,851	£7,840
Non-Staff at NGS and OMII				
Travel and expenses NGS		£500	£250	£750
Travel and expenses OMII		£500	£250	£750

Total Non-Staff (B)		£1,000	£500	£1,500
Directly Incurred Total (A+B=C)		£11,543	£6,524	£18,067
Directly Allocated NGS		£851	£486	£1,337
OMII		£3,070	£1,754	£4,824
Indirect Costs (E) NGS		£5,750	£3,286	£9,036
OMII		£6,225	£3,557	£9,782
Total Project Cost NGS and OMII		£27,439	£15,607	£43,046
Total Project Cost	£13,410	£167,245	£44,389	£225,045
Amount Requested from JISC	£10,728	£111,845	£23,026	£145,599
Institutional Contributions	£2,682	£55,400	£21,363	£79,446
Percentage Contributions over the life of the project		JISC 65 %	Partners 35%	Total 100%

10.1 To ensure the project achieves all of its objectives, we seek funding for two researchers: one at Kent and the other at NeSC for 13.5 man months and 9 man months respectively. The 2.75 man months for personnel at NGS will be funded by the NGS. Given the requirements for a high level of computing and modeling expertise, experienced researchers with a high level of IT competence are required. The researchers will undertake a significant amount of travel, to interact with the collaborating establishments, to attend quarterly meetings, and to widely disseminate the work both nationally and internationally at conferences such as UK e-Science All Hands Meeting, TERENA TNC, IEEE Grid and/or Cluster Computing Grid (CCGrid).

10.2 We believe that this project represents good value for money due to the expertise that the project partners bring, the contributions we are making to the costs and importantly the variety of on-going and significant e-Science projects upon which we will capitalize. The researchers will be supported by other researchers at the NGS, NeSC and Kent who will contribute their efforts to ensure that the overall goals of the project are realized. This represents a unique and cost effective opportunity to integrate leading security technologies to enhance the management and security of grids and improve the overall security of national resources such as the NGS.

11. Impact

11.1 Providing both organisational and VO users with the same privilege management mechanisms and policy management tools will provide synergies and cost savings through reduced learning times, less complexity, lower management overheads and integrated infrastructures. The use of standard interfaces and protocols will also make it easier to plug and play additional components, reducing costs even further. Appendix C illustrates how this ability can be further demonstrated in this project.

11.2 Long term sustainability is ensured in several ways. The NGS will run the VOMS and PERMIS services on behalf of the whole community, and provide first level support to users. The PERMIS software is open source and so is available for anyone to adapt, update and bug fix, but more importantly, since PERMIS is being integrated into the OMII-UK software release, the latter has a long term commitment to the UK community to commission the hardening, maintenance and support of software components that are useful and being used by the UK e-Science community. Kent will also continue to provide support to integrators and to enhance PERMIS with new features within the context of its ongoing and future R&D projects. The PERMIS web site lists a number of these projects as well as new ideas for continuing R&D work in authorisation infrastructures.

12. Risk Assessment

12.1 Reliance on other projects. This primarily affects the OMII-UK demonstrator (but not the GT4 or Shibboleth demonstrators). We are reliant on LESC integrating PERMIS within the OMII-UK software release and releasing it in time for the second demonstrator. This is low risk (as the expected delivery date is April 2007 and WP4 is not scheduled to start until August 2007) but high impact. We are reliant on VOMS producing a SAML interface for the open retrieval of its attributes for the OMII-

UK demonstrator. This is low risk (as the notified release date for the first working prototype is April 2007) but again high impact. We are reliant on the OGF completing the specification of the 2nd generation OGSA AuthZ protocols and on OMII-UK implementing them. As the publication date is not fixed, and the full demand from the community for these protocols cannot be assessed by OMII-UK at this time, OMII-UK cannot give a firm commitment today on implementing these extensions into its software in time for this project (see Letter of Support). This is high risk but low impact. *Contingencies.* As the PI is joint chair of the OGSA AuthZ WG and joint editor of the 2nd generation AuthZ profiles he can have some influence over their timely production. As Prof Sinnott is a member of the OMII-UK Users' Forum the requirement has already been fed into OMII-UK. If OMII-UK do not implement (or subcontract) the 2nd generation protocol in time, we can still perform the OMII-UK demonstrator using the existing 1st generation protocol, but this will mean that some authorisation policies cannot be tested (i.e. ones that have conditions on operation arguments).

12.2 Beating the March 2009 Deadline. This is a hard deadline for JISC by which date all projects must be finished. This is very low risk and low impact to our project. We have a 13.5 month project which we have scheduled over 17 months so as to build sufficient contingency into the plan. We still have 8 months after the scheduled completion date to beat the March 2009 deadline.

12.3 Biased reporting: In a software development activity it is important to have unbiased evaluation based on application/user pull as opposed to middleware push. By having NeSC as the project partner responsible for the demonstrations, one can be assured that they will specifically feed the positive and negative results of the demonstrators into the UK e-Science and OMII-UK user groups. They will report on the benefits of VOMS versus Shibboleth versus PERMIS DIS for attribute provision, and PERMIS vs. XACML for PDP access control decision making. They will take into account the ease at which the overall solution can be used and managed by the NGS and other VO managers, and importantly, how easy it is for developers to use the solutions and integrate them into their applications. They will also be guided by advice from JISC and the wider security research community in their efforts. Both NeSC and NGS do not produce middleware, but have an entirely application and service oriented focus. This project will draw directly on their experience without additional requirements for more resources. NeSC currently use numerous different Grid middleware including Globus (versions 2, 3 and 4), Condor, OMII-UK, OGSA-DAI, GridSphere, WebSphere, and have explored a wide array of authorisation infrastructures including PERMIS, GSI and CAS, and their various versions. Thus we believe that the risk of biased reporting is very low risk.

12.4 Application Domain Specific Solutions: With some projects there exists the danger that the solutions are applicable to only one domain and not another, but this is low risk. Through the rich portfolio of application projects at NeSC, we will fully explore the VOMS-PERMIS software and fully analyse it against existing solutions. Through a depth of knowledge in tools and techniques for establishing and managing VOs, NeSC are well placed to ensure software developed meets the e-Research community needs and is not tied to one application specific domain.

12.5 Failures in Project Management: Project management is a critical success factor for any IT project, so failure is usually high impact. Problems can especially arise in co-ordination of work when distributed teams are involved. However this project is low risk since the PIs at Kent and NeSC already have a strong track record of successfully delivering their own projects as well as a significant joint project (DyVOSE). Excellent channels of communication and working processes are already in place between the PIs and their teams. The PIs enjoy a good rapport with each other, and understand each others modes of working and strengths and weaknesses. Thus it is anticipated that they will be able to adequately resolve any PM issues that arise during the course of this project.

12.6 Resource Limitations - Staff: Staff are a critical resource for any project. Failures can be high impact. For this project it is a low risk since both Kent and NeSC have established teams of RAs. Thus if any single team member is not available, another one is usually there to take their place. At Glasgow the work will primarily be undertaken by Mr Jipu Jiang and Dr John Watt under the direct supervision of Prof. Sinnott. Mr Jiang/Dr Watt have an extensive track record in Grid technologies, portal technologies such as GridSphere and WebSphere, Shibboleth and authorisation technologies such as PERMIS, GSI and associated solutions such as MyProxy. Both are actively involved in the GLASS project and are helping to Shibboleth-enable numerous services at Glasgow University,

building upon the unified account management system at Glasgow. These experiences will directly shape the Shibboleth explorations in this project. In addition to Mr Jiang, Dr Watt and Prof. Sinnott NeSC will draw on the efforts of the various RAs at Glasgow involved in the applications identified previously. The RAs associated with these projects at NeSC have extensive experience in GT2, GT4 and OMII-UK technologies (including the OMII-UK software with its OGSA-DAI and myGrid components) and will provide extensive support to ensure the successful delivery of the various case studies in WP5. At Kent the work will be undertaken by several different RAs: Mr Linying Su, who is adding coordination between multiple PDPs as a new service for GT4 and PERMIS; Mr Christian Azzopardi who is the author of the PERMIS Policy ManagerV2 and Policy Wizard, Mr Tuan Ahn Nguyen who is the author of the PERMIS DIS, and Mr George Inman who is supporting Shibboleth.

12. Key Personnel

12.1 Professor David Chadwick is the leader of the Information Systems Security Research Group (ISSRG) at the **University of Kent**. He has written over 80 books, chapters, journal and conference papers, mostly about security, and the latest of these can be downloaded from <http://www.cs.kent.ac.uk/people/staff/dwc8/pubs.html>. He has been the principal investigator in over 25 research grants from a variety of sources including the EPSRC and the EC. He has participated in 5 previous Grid related JISC funded security projects including DyVOSE (led by NeSC at Glasgow); DyCOM (led by Kent, partnered by CCLRC); and FAME-PERMIS (led by the University of Manchester). The results of these have been widely demonstrated and made available to the global community as open source software under the BSD license. Professor Chadwick was a member of the EPSRC e-Science Security Taskforce, is still the BSI lead representative to ISO/ITU-T X.500 standards meetings which include X.509 PKIs and PMIs, the basic technologies used in Grid security. He is co-author of the GGF OGSA SAML Authorisation profile, and co-chair of OGSA-AUTHZ working group. He is the chief architect and designer of the PERMIS software, which is now part of the public US NMI Internet2/Grid software release and is integrated with Globus Toolkit, Shibboleth and Apache. It is the only freely available open source X.509 based PMI toolkit in the world today.

12.2 Professor Richard Sinnott is the Technical Director for **The National e-Science Centre (NeSC)** at the University of Glasgow. He has led a range of Grid security projects including DyVOSE, BRIDGES, ESP-Grid, GEMEPE, GEODE, GLASS, VOTES, GHI, nanoCMOS, SBRN and UK e-Science ETF projects (see www.nesc.ac.uk/hub/projects). All of these projects are concerned with security, with BRIDGES, DyVOSE, ESP-Grid, ETF, nanoCMOS and SBRN concerned particularly with the security issues and solutions associated with HPC-based access to Grid infrastructures. Within the BRIDGES project he led the implementation of solutions showing how an advanced authorization infrastructure based upon PERMIS can be used to provide both data security and compute security. Drawing on this pool of highly relevant Grid security focused projects makes Prof Sinnott an ideal person to lead the 3 demonstrators of this project. Professor Sinnott has a broad background in open distributed processing systems and has acted as editor for numerous international standards in this area.

12.3 Dr Andrew Richards is the executive director and technical manager of the **National Grid Service (NGS)** which was established in 2004 to provide a dedicated and reliable Grid infrastructure for e-Scientists across the UK. The NGS comprises two HPC compute clusters and two data clusters across four sites in the UK. Other e-Science centres are in the process of integrating their own local compute resources into this fabric. Through the involvement of NGS we will gain valuable first hand feedback on the practical aspects of deploying Grid security solutions in a real, large scale context.

12.4 Dr Stephen Newhouse is Director of the **Open Middleware Infrastructure Institute UK**, a collaborative e-Science project between the University of Southampton, the University of Edinburgh, and the University of Manchester. He is a member of the Open Grid Forum (OGF) Steering group, where he is responsible for Application Standards, and is on the management or oversight boards of the National Grid Service (NGS), AstroGrid and GridPP. He remains active in the Open Grid Services Architecture Working Group (OGSA-WG) of the OGF. Before moving to Southampton in June 2004 he was the Sun Lecturer in e-Science in the Department of Computing at Imperial College London and Technical Director of the London e-Science Centre (LeSC) (<http://www.lesc.ic.ac.uk/>).

Appendix A

References

- [1] Alfieri, R., Cecchini, R., Ciaschini, V., Dell'Agnello, L., Frohner, A., Lorente, K., Spataro, F., *From gridmap-file to VOMS: managing authorization in a Grid environment*, Future Generation Computer Systems. Vol. 21, no. 4, pp. 549-558. Apr. 2005
- [2] D.W. Chadwick, A. Otenko *The PERMIS X.509 Role Based Privilege Management Infrastructure*. Future Generation Computer Systems, 936 (2002) 1–13, December 2002. Elsevier Science BV.
- [3] V. Welch, R. Ananthakrishnan, F. Siebenlist, D. Chadwick, S. Meder, L. Pearlman, *Use of SAML for OGSIA Authorization*, Aug 2005, Available from <https://forge.gridforum.org/projects/ogsa-authz>
- [4] OASIS. *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS Standard, 15 March 2005.
- [5] OASIS. *eXtensible Access Control Markup Language (XACML) Version 2.0*, OASIS Standard, 1 Feb 2005
- [6] VOMS home page: <http://hep-project-grid-scg.web.cern.ch/hep-project-grid-scg/voms.html>
- [7] ISO 9594-8/ITU-T Rec. X.509 (2001) The Directory: Public-key and attribute certificate frameworks
- [8] Steenbakkens, M., Guide to LCAS version 1.1.16, <http://hep-proj-grid-fabric.web.cern.ch/hep-proj-grid-fabric/documentation/lcas.pdf>
- [9] S. Brostoff, M. A. Sasse, D. Chadwick, J. Cunningham, U. Mbanaso, A. Otenko. *R-What? Development of a Role-Based Access Control (RBAC) Policy-Writing Tool for e-Scientists* Software: Practice and Experience, Volume 35, Issue 9, Date: 25 July 2005, Pages: 835-856
- [10] Chadwick, D.W., Novikov, A., Otenko, O. *GridShib and PERMIS Integration*. Terena Networking Conference (TNC 2006), Scicily, May 2006.
- [11] Chadwick, D.W., *Delegation Issuing Service*, in NIST 4th Annual PKI Workshop, pages 62-73, Gaithersberg, USA, April 2005.
- [12] R.O. Sinnott, *Initial Experiences in Developing e-Health Solutions across Scotland*, Workshop on Integrated Health Records: Practice and Technology, Edinburgh, March 2006.
- [13] 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.
- [14] R.O. Sinnott, O. Ajayi, A.J. Stell, *Secure Federated Data Retrieval in Clinical Trials*, Telemedicine 2006 conference, Banff, Canada, July 2006.
- [15] R.O. Sinnott, O. Ajayi, A.J. Stell, *Supporting the Clinical Trial Recruitment Process Through the Grid*, Nottingham UK e-Science All Hands Meeting, September 2006.
- [16] D. Chadwick, G. Zhao, A. Otenko, R. Laborde, L. Su, T.A. Nguyen. *Building a Modular Authorization Infrastructure*, presented at All Hands Meeting, Nottingham, Sept 2006.
- [17] See <http://infnforge.cnaf.infn.it/gpbox/>
- [18] 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.
- [19] R.O. Sinnott, A. Asenov, D. Berry, S. Furber, C. Millar, A. Murray, S. Pickles, S. Roy, A. Tyrell, M. Zwolinski, *Meeting the Design Challenges of nanoCMOS Electronics: An Introduction to an EPSRC Pilot Project*, UK e-Science All Hands Meeting, Nottingham UK, September 2006.
- [20] D. W Chadwick, A. Otenko and T.A. Nguyen. *Adding Support to XACML for Dynamic Delegation of Authority in Multiple Domains*, to be presented at IFIP CMS 2006, October 2006
- [21] W. Xu, D.W. Chadwick, A. Otenko. *Development of a Flexible PERMIS Authorisation Module for Shibboleth and Apache Server*, Proceedings of 2nd EuroPKI Workshop, University of Kent, July 2005
- [22] See <http://middleware.internet2.edu/signet> and <http://middleware.internet2.edu/dir/groups/grouper>
- [23] See <http://sec.cs.kent.ac.uk/permis>
- [24] D.W. Chadwick, L. Su. *Use of WS-Trust and SAML to access a CVS*. OGSA-Authz WG Draft Standard. 12 April 2006.
- [25] D.W. Chadwick, L. Su, R. Laborde. *Use of XACML Request Context to access a PDP*. OGSA-Authz WG Draft Standard. 28 March 2006.

Appendix B

FOI Withheld Information Form

We would like JISC to consider withholding the following sections or paragraphs from disclosure should the contents of this proposal be requested under the Freedom of Information Act.

We acknowledge that the FOI Withheld Information Form is of indicative value only and that JISC may nevertheless be obliged to disclose this information in accordance with the requirements of the Act. We acknowledge that the final decision on disclosure rests with JISC.

Section / Paragraph No.	Relevant exemption from disclosure under FOI	Justification
NONE		

Please see <http://www.ico.gov.uk> for further information on the Freedom of Information Act and the exemptions to disclosure it contains.

Appendix C

Interaction between VPMAN, Shintau and nDoA

Technical

The main objective of VPMAN is to integrate the VOMS user management and attribute assignment function with the PERMIS policy based authorisation decision function. The main software objective of Shintau is to develop a Policy Information Point (the nAA-PIP) that can aggregate and validate the attributes assigned by multiple attribute authorities. The main objective of nDoA is to enable n-tier delegation of authority between web services and/or people. All three projects complement each other as described below.

VPMAN and Shintau. The three demonstrators of VPMAN will only collect attributes from a VOMS server and use these to make authorisation decisions. The Shib, OMII, GT2 and GT4 demonstrator of VPMAN will use Shibboleth for authentication, and attributes from VOMS for authorisation, but still won't use attributes from multiple authorities for authorisation. However, once the nAA-PIP from Shintau is developed, this will be able to be seamlessly plugged into the VPMAN infrastructure using existing interfaces and allow PERMIS to make authorisation decisions based on attributes from VOMS servers and from other attribute authorities such as Shibboleth IdPs, professional certifying authorities such as the General Medical Council and learned societies such as the IEEE and the ACM.

VPMAN and nDoA. Globus Toolkit already has a functioning n-tier delegation architecture based on proxy certificates. This is limited in that it only delegates from a user to his job, nevertheless it is sufficient for the Globus Toolkit demonstrator in VPMAN. N-tier delegation of authority between users is handled by the existing PERMIS DIS service piloted in the DyVOSE project. OMII currently does not have an n-tier delegation capability. Its n-tier processing relies on the next tier trusting the previous tier to have performed the correct checks on the user, and therefore the previous tier is trusted to do anything on the next tier. The n-tier delegation of authority planned in nDoA will make a welcome addition to the OMII infrastructure and provide a constrained delegation capability thus limiting the trust that the next tier has to place in the preceding tier.

nDoA and Shintau. These two projects add orthogonal and complimentary capabilities to the VPMAN infrastructure. nDoA allows one service or person to delegate attributes to another service or person, whilst Shintau allows a set of attributes for a person or service to be collected from different IdPs and validated prior to access control decision making. They will not directly interact with each other unless the policy of the nAA-PIP allows delegation of authority by its trusted IdPs. Note the PERMIS CVS already allows this capability, as it was introduced in the DyVOSE project. When the IdPs delegation policy is enhanced in nDoA, the validation mechanism in the nAA-PIP will also need enhancing, but this has been planned for in the nDoA project. Note that when an IdP holds attributes that have been delegated internally from one user to another (by nDoA, Signet, Grouper or any other delegation capability) this will be transparent to Shintau if all the credentials are issued by the IdP in question, in which case a knowledge of the delegation history prior to credential issuing is either hidden or not relevant to the credential validation capability of Shintau. If one web service delegates to another web service, and the nAA-PIP of the second web service then either pulls or is pushed the credentials of the requestor (whether from one IdP or several), this delegation may or may not be relevant to the attribute collection and validation undertaken by the nAA-PIP, depending upon its validation policy.

Financial and Managerial

All three projects are scheduled to run in parallel, with Shintau being longer than the other two. The technical implementation for VPMAN and nDoA is scheduled at the start of the projects with the

piloting towards the end. Shintau on the other hand is scheduled so that the start of the project (first year) is low intensity long duration protocol design involving multiple iterations with technical staff around the globe. The high intensity implementation work of Shintau starts after the implementation work of VPMAN and nDoA has completed, therefore the same technical staff at Kent can be used to implement Shintau once they have finished implementing VPMAN and nDoA. The benefits of this synergy have been built into the Shintau project plan.

The piloting in VPMAN and nDoA is being performed by NeSC. We were keenly aware of JISC's tight financial constraints when producing the budgets for these projects. Therefore we have described more application scenarios in the nDoA proposal than we have costed for demonstrating. Thus if both projects were to be funded, we would hope to be able to add an additional application domain to the nDoA demonstrations.

The piloting in Shintau has not been determined yet, and no costs have been directly attributed to this in that proposal. Therefore there cannot be any cost savings in the piloting phase of Shintau.

Valerio Venturi
INFN CNAF
viale Berti Pichat 6/2
40127 Bologna Italy
valerio.venturi@cnafe.infn.it
+390516092800

Bologna, November 5 2006

Dear David,

thank you for sending me a copy of your proposal entitled "Integrating VOMS and PERMIS for Superior Secure Grid Management". Being convinced that modularity, replaceability and interoperability are key features for security components in highly dynamic context such as grids, we are pleased that you are deciding to integrate PERMIS with VOMS. We support your proposal and wish you the best of success. We plan to have a SAML interface to VOMS available for alpha testing in April 2007, and we will be happy to let you have the software when you are ready to use it.

Yours sincerely,

Valerio Venturi



open middleware
infrastructure
institute uk

c/o Suite 6005, Faraday Building (B21),
Highfield Campus, Southampton University,
Southampton, SO17 1BJ

Telephone: +44 (0)2380 598789

Email: s.newhouse@omii.ac.uk

Dr Steven Newhouse, Director

Dear David,

OMII-UK is pleased to support your proposal entitled "Integrating VOMS and PERMIS for Superior Secure Grid Management". Concerning the integration of an Authorisation service into the OMII-UK software environment that uses PERMIS, work is progressing well and we expect to have the first version available before April 2007. We will be happy to let you have prototypes of this integration for your project as soon as it is ready.

We will be tracking the next generation protocols emerging from the OGSA-Authz Working Group in the OGF. We cannot commit to implementing these at this time, nor can we commit to integrating the software into our public release, as we are unable to assess the compatibility of other infrastructures with this protocol, the demand from the community for this capability or the quality of this code. As your software becomes available I would welcome feedback from the community to help us assess the prioritisation of this work.

Yours sincerely

Steven Newhouse
Director, OMII-UK

UNIVERSITY
of
GLASGOW



Joint Information Systems Committee (JISC)
JISC Executive
Northavon House
Coldharbour Lane
Bristol BS16 1QD

11th November 2006

Re: Integrating VOMS and PERMIS for Superior Secure Grid Management (VPMAN)

Dear Mr Farnhill,

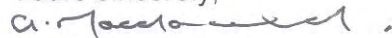
As Director for IT at the University of Glasgow I am happy to offer my strong support for this proposal looking at integrating VOMS and PERMIS. At Glasgow we have a body of experience in many Grid-related application domains. We lead for example the GridPP2 project (Prof Tony Doyle project manager); we are directly involved in the UK e-Science Grid (with researchers directly involved in the Engineering Task Force) and we are currently involved in making resources available to the NGS (based upon a provisional 10% of our newly procured £800k cluster and other HPC clusters available at Glasgow). Furthermore through Prof Sinnott we have a range of Grid-based projects across the e-Research spectrum (clinical, engineering, biomedical, social, arts and humanities), many of which have exploited the PERMIS

technology.

For the longer term, it is crucial that there are common technologies and processes that allow Grid resources and applications to work together across the numerous research domains identified above. This proposal is an important step to achieving this. Through integration of PERMIS and VOMS the ability to specify security attributes associated with virtual organisations ala VOMS (which has considerable uptake by the Grid community), and subsequently use them (via PERMIS) to make fine grained authorisation decisions will be realised. This will directly shape UK-wide efforts where for example the NGS are looking at rolling out VOMS. We also expect this to be of benefit to the Scottish Grid Service which will be complimentary and interoperable with the NGS. The results will also impact on international Grid efforts in this area, e.g. within the EGEE project which is now moving towards research domains where finer grained security models are required.

Strategically I regard this proposal as important for Grid efforts in Scotland, but perhaps more importantly for the UK and wider Grid communities more generally. As Director of IT Services at the University of Glasgow, I fully support this proposal and am happy to see my staff involved in ensuring that it achieves its objectives.

Yours sincerely,



Sandy Macdonald
Director of IT Services

Mr Sandy MacDonald – Director of IT Services

James Watt (North) Building, University of Glasgow, Glasgow G12 8QQ

Telephone: 0141 330 4860 Fax: 0141 330 4850 Email: a.macdonald@admin.gla.ac.uk



National Grid Service
Grid Operations and Support Centre
CCLRC e-Science Centre
Rutherford Appleton Laboratory
Chilton
Didcot
Oxfordshire
OX11 0QX

David Chadwick
Computing Laboratory
University of Kent
Canterbury
CT2 7NF

I am writing on behalf of the National Grid Service in support of the ‘Integrating VOMS and PERMIS for Superior Secure Grid Management (VPMAN)’ project. The NGS will be happy to contribute in supporting the VPMAN project on the use of the National Grid Service as detailed in the project proposal.

The remit of the National Grid Service is to provide a service for all UK academics and to engage with a variety of disciplines and communities. We believe providing secure authentication and authorisation mechanisms for access is essential for the development of the NGS service.

Yours Sincerely

Dr Andrew Richards
Executive Director, National Grid Service

Simon Thompson

Director and Professor of Logic and Computation

Tel: +44 1227 823820

Fax: +44 1227 762811

Email: S.J.Thompson@kent.ac.uk

Web: <http://www.cs.kent.ac.uk/~sjt/>

JISC e-Infrastructre bids
einfastructure-bids@jisc.ac.uk

20 November 2006

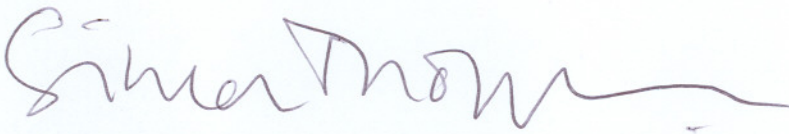
Dear Sir or Madam,

VPMan Proposal

The University of Kent strongly supports the proposal Integrating VOMS and PERMIS for Superior Secure Grid Management (VPMan) led by Professor Chadwick. This proposal will integrate together two important components for Grid security management, namely VOMS from INFN, Italy, and PERMIS from our own laboratory. We are pleased to support Professor Chadwick in leading this work, and welcome his collaboration with the National Grid Service, OMII (UK), the National eScience Centre at Glasgow and INFN in Italy. We are sure that his experiences from working in many multiparty research consortia will enable him to manage this project effectively.

We are glad that Professor Chadwick's team in the Information Systems Security Research Group will lead the implementation of this integration and we will ensure that they have the necessary resources to do this. We will also support the global distribution of the open source code from our department's web server, once it has been implemented.

Yours faithfully,



Prof Simon Thompson
Director, Computing Laboratory