



## JISC Completion Report

Project Information			
<b>Project Acronym</b>	VPMan		
<b>Project Title</b>	Integrating <u>V</u> OMS and <u>P</u> ERMIS for Superior Secure Grid <u>M</u> anagement		
<b>Start Date</b>	1 March 2007	<b>End Date</b>	31 July 2008 -> 30 April 2009
<b>Lead Institution</b>	University of Kent		
<b>Project Director</b>	Professor David Chadwick		
<b>Project Manager &amp; contact details</b>	Dr Hani Ragab-Hassen University of Kent, Computing Laboratory, Canterbury, CT2 7NF. Email: H.Ragab@kent.ac.uk Mobile: +44 1227 82 3816		
<b>Partner Institutions</b>	The National e-Science Centre (NeSC) at the University of Glasgow ( <a href="http://www.nesc.ac.uk/">http://www.nesc.ac.uk/</a> ) The National Grid Service at the Science and Technology Facilities Council ( <a href="http://www.grid-support.ac.uk/">http://www.grid-support.ac.uk/</a> ) Open Middleware Infrastructure Institute UK ( <a href="http://www.omii.ac.uk/">http://www.omii.ac.uk/</a> )		
<b>Project Web URL</b>	<a href="http://sec.cs.kent.ac.uk/vpman/">http://sec.cs.kent.ac.uk/vpman/</a>		
<b>Programme Name (and number)</b>	e-Infrastructure (security)		
<b>Programme Manager</b>	Christopher Brown		

Document Name			
<b>Document Title</b>	Completion Report		
<b>Reporting Period</b>			
<b>Author(s) &amp; project role</b>	David Chadwick (Project Director), Richard Sinnott (Glasgow PI), Andrew Richards (NGS Manager), Neil P Chue Hong (OMII-UK Director)		
<b>Date</b>	9 January 2010	<b>Filename</b>	VPManCompletionReport.doc
<b>URL</b>	<a href="http://sec.cs.kent.ac.uk/vpman/VPManCompletionReport.pdf">http://sec.cs.kent.ac.uk/vpman/VPManCompletionReport.pdf</a>		
<b>Access</b>	<input type="checkbox"/> Project and JISC internal	<input checked="" type="checkbox"/> General dissemination	

Document History		
Version	Date	Comments
0.9	25 Aug 2009	Final Draft for Review
1.0	9 January 2010	Final Report



## JISC Completion Report (2009)

### *Project Sign-off*

#### **1. Project Outputs**

The project deliverables that were specified in the project proposal and project plan are listed below, along with the titles of the actual deliverables

##### **Deliverables**

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

Delivered *"Integrating VOMS and PERMIS for Superior Secure Grid Management (VPman), Deliverable 1.1, Requirements and information gathering" Version <1.0> 11 July 2007*

**D1.2** A document of case studies to be supported

Delivered *"Integrating VOMS and PERMIS for Superior Secure Grid Management (VPman), Deliverable 1.2, Use cases", Version <0.5> 16 July 2007*

**D2.1** A VOMS-PERMISS integration design document.

Delivered *"Integrating VOMS and PERMIS for Superior Secure Grid Management (VPman), Deliverable 2.1, VOMS - PERMISS Integration design document", Version <1.0>, 10 April 2008*

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

Delivered *"PERMISS Policy Editor, v5.0, 9 Oct. 2008*

**D4.1** Beta software ready for validation and piloting.

Delivered PERMISS/GT4 software to Glasgow in July 2007. OMII/PERMISS software was never delivered to Glasgow for testing, but Glasgow built a proof of concept test case showing how OMII-UK services (GridSAM) could be protected using VOMS attributes directly.

**D4.2** Preparation of test bed, services and portals

Delivered. Glasgow built the test bed during 2007.

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

Delivered *R.O. Sinnott, D.W.Chadwick, T. Doherty, D. Martin, A. Stell, G. Stewart, L. Su, J. Watt. "Advanced Security for Virtual Organizations: The Pros and Cons of Centralized vs Decentralized Security Models". Proc. 8th IEEE International Symposium on Cluster Computing and the Grid (CCGrid 2008). May 19-22, 2008, Ecole Normale Superieure de Lyon, Lyon, France.*

**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.

Delivered *R.O. Sinnott, A. Asenov, C. Bayliss, C. Davenhall, T. Doherty, B. Harbulot, M. Jones, D. Martin, C. Millar, G. Roy, S. Roy, G. Stewart, J. Watt. "Integrating Security Solutions to Support nanoCMOS Electronics Research". IEEE International Symposium on Parallel and Distributed Processing Systems with Applications, Sydney Australia, December 2008.*

**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)

### **Not Yet Delivered.**

*Note. Since the final integrated software was never put into operation at the NGS, all that the NGS can produce is a report on the use of PERMIS as part of the SARoNGS project.*

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

1. The PERMIS/GT4/VOMS download is available from  
<http://sec.cs.kent.ac.uk/permis/integrationProjects/GT.shtml>

and the actual software is at  
[http://sec.cs.kent.ac.uk/permis/private/gt4/permisAuthzGT4\\_5\\_1\\_0.zip](http://sec.cs.kent.ac.uk/permis/private/gt4/permisAuthzGT4_5_1_0.zip)

2. The OMII-AuthZ 1.0.0 is downloadable in source code form from the OMII-UK website  
<http://www.omii.ac.uk/wiki/Downloads>.

However OMII-UK cannot recommend it for production use at this time until the outstanding bug in the BouncyCastle interceptor code is fixed.

**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.

Delivered

1. The PERMIS/GT4/VOMS documentation is at  
[http://sec.cs.kent.ac.uk/permis/documents/PERMIS\\_Authorization\\_in\\_GT4.pdf](http://sec.cs.kent.ac.uk/permis/documents/PERMIS_Authorization_in_GT4.pdf)

2. The OMII-AuthZ 1.0.0 is downloadable in source code form from the OMII-UK website  
<http://www.omii.ac.uk/wiki/Downloads>.

**D6.3** Final report to JISC  
Delivered "VPMan Final Report", v1.0, 29 July 2009

## **2. Intellectual Property Rights**

We confirm that there are no IPR issues that prevent the project outputs from being made available to the teaching, learning, and research communities now that the project has ended.

We confirm that all necessary permissions for third-party IPR have been granted. The permission from IAIK to use their binaries, which are included in the PERMIS binary releases, for research and educational purposes, can be found here  
<http://sec.cs.kent.ac.uk/permis/essentials/permislicence.shtml>.

The license for the OMII-AuthZ code is bundled with the source code, as is the BSD-like license for all the PERMIS open source code.

## **3. Project Staff**

Dr Bassem Nasser, University of Kent, worked on the project for the first 7 months then moved to a permanent post at the IT Innovation Centre, Southampton.

Linying Su, University of Kent (full time), worked on the project after Bassem left, and has now returned to the Inner Mongolia University in China to continue his career there at an enhanced level.

Dr Hani Ragab Hassen is a lecturer at the University of Kent and was project manager after Dr Nasser left.

Professor David W Chadwick is a professor at the University of Kent.

Mr David Martin is a systems administrator and server manager at the University of Glasgow. He has over 30 years experience working with large scale compute clusters and a variety of Grid middleware.

Mr Tom Doherty is a Grid Engineer employed at NeSC (50%) and in the Department of Physics (50%) at the University of Glasgow. Both David and Tom continue to work at Glasgow on a range of Grid and campus-oriented projects.

The following staff from the NGS contributed to the project

Andrew Richards  
Mike Jones  
Jens Jensen  
Xiaodong Wang

The OMII-UK members of the project staff were:

Dr Stephen Crouch, an Architect at OMII-UK, University of Southampton.  
Dr Hugo Mills, OMII-UK Southampton, who has recently taken up a position as a Research Fellow at ACET, University of Reading  
Dr Neil P Chu Hong, the director of OMII-UK

## 4. Dissemination Plan

1. The project has produced two conference publications as listed above and numerous related publications as listed in Appendix A.
2. The project has a web site at <http://sec.cs.kent.ac.uk/vpman/>
3. The project ran several public demonstrations as described in the Final Report.
4. The project has made the PERMIS software freely available as both open source code (<http://www.openpermis.org>) and as binary files that are ready to run (<http://sec.cs.kent.ac.uk/permis/downloads/download.shtml>).
5. The project has made the OMII-UK Authz software available from the OMII-UK web site.

## 5. Exit Plan

The University of Kent has several web sites for disseminating the project outputs as described above.

- i) We confirm that the University of Kent will continue to host the VPMAN project and PERMIS web sites for 3 years after the project end date and will assist JISC in archiving it subsequently.

In addition to the above, the SWISS Ministry of Defence has re-engineered and hardened the core of the PERMIS software and has made this publicly available at <http://www.osor.eu/projects/openpermis>. Since this software is being used in a military application, it is likely that the SWISS MoD will continue to support this version for the foreseeable future.

OMII-UK hosts information about e-Science related software.

- i) We confirm that OMII-UK will continue to host the source code for the OMII-AuthZ software and maintain the GridSAM codebase hosted at Sourceforge for 2 years after the project end date and will assist JISC in archiving it subsequently.

## 6. Sustainability Plan

PERMIS is continuing to be developed by the University of Kent under the EC TAS3 project. The core of PERMIS has also been commercially hardened by the SWISS Ministry of Defence for a military application and this software is being published and maintained as open source software at OSOR web site.

Other commercial companies are using PERMIS and downloads are currently running at several hundred per month. It is likely that other initiatives will emerge in the coming months which will continue to sustain and further develop the PERMIS software suite.

## **7. Budget**

The project did not receive funds from other sources than JISC, but it should be noted that both OMII-UK and the NGS used their own resources to contribute to this project. The final expenditure vs. budget is provided in Appendix B for both the University of Kent and the NeSC, Glasgow.

## ***Lessons Learned***

### **8. Aims and Objectives**

The project achieved all its stated objectives apart from integrating the final software in a pilot operational system at STFC. This is most likely due to the project partners having some misaligned objectives. VPMAN was originally conceived so that the NGS would take the software developed by the University of Kent and deploy it as a prototype. However, the NGS now say that it was never their objective to use PERMIS at any point (although Kent was not aware of this). The NGS only had a requirement to make AuthZ work; and indeed it was not supposed to be developing any middleware of its own. Given that LCAS/LCMAPS already existed and tuned more readily towards the NGS grid AuthZ requirements, by providing a user id/guid module that told the operating system which username to run the grid job under, it was much easier to plug this into the NGS and so that's what the NGS focussed on. The NGS expected that VPMAN would provide a similar authz functionality along with an operating system module for running a grid job under a particular uid/guid and they were keen to test it, but no such user id obligation module was provided by Kent. This is because Kent expected the application to handle any returned obligations once PERMIS had returned the authz result saying that the user was granted access to run the job under a given uid/guid. Hence the bit of glue that took the returned guid/uid obligation and enacted it for the operating system was never built or tested by any partner.

### **9. Overall Approach**

Ideally the project should have been managed by STFC since they were the ultimate beneficiaries of the project's deliverables. STFC were the only partners capable of installing the completed software and offering a pilot service to their users. As it was, with the University of Kent managing the project, it felt a little bit like the tail trying to wag the dog. With hindsight, STFC now realise that they should have put in the bid themselves, and should have included payments to STFC staff in the proposal.

### **10. Project Outcomes**

There is nothing further to add to the Final Report.

### **11. Stakeholders**

The potential beneficiaries are grid users, developers and administrators. Providing grid administrators and users with the same authorisation 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 between the authorisation infrastructure and grid middleware also makes it easier to plug and play additional components, reducing costs even further, and avoiding lock-in to specific products.

The results of the project have been used to influence a range of projects at NeSC Glasgow directly. It remains a non-trivial exercise for others to simply adopt the solutions however, i.e. without the depth of knowledge in setting up and configuring the associated technologies.

As a deployment (as opposed to development) stakeholder, OMII-UK would probably have benefited from a closer interaction between the VPMAN and SARONGS projects so that the deliverables could have been used in more of their application focussed projects and ultimately made better use of the NGS facilities.

## 12. Project Partners

The directly funded partners in the project were:

- The University of Kent.
- The National E-Science Centre at the University of Glasgow.

The self funded partners in the project were

- The UK National Grid Service (STFC)
- Open Middleware Infrastructure Institute (OMII-UK)

In addition the project had direct links with

- Instituto Nazionale di Fisica Nucleare (INFN), Italy, who were developing a new VOMS attribute pull module to be used by the project.

and indirect links with

- The Universities of Manchester, via the SARoNGS project,
- The University of Oxford, via the SARoNGS project,
- The London e-Science Centre (LeSC) who were subcontractors to OMII-UK.

It is difficult, when a project has several unpaid partners, to get the same level of commitment from them as from the paid partners. This is quite natural, since the unpaid partners will have paid projects of their own that they will have to devote their time and efforts to. One could therefore say that the project was structurally flawed at conception, due to the different commitment levels of the different partners. However, the unpaid partners cannot be held responsible for a lack of project management or changing staff that accounts for why the project did not deliver on time.

## 13. Project Management

The project suffered from a number of project management weaknesses, which were documented in the Final Report. These are not repeated here. This project also suffered from not having an experienced proactive project manager for the duration of the project. The first project manager left after seven months and the second project manager did not have all the required attributes. Ultimately the project director, Professor Chadwick, must take full responsibility for this lack of effective project management.

## 14. Programme Support

The project that OMII-UK subcontracted to LeSC had a direct impact on this project, as this project required its output. The LeSC project was very late in delivering and never did deliver fully debugged code before the end of this project.

The INFN project had a direct impact on this project as its deliverables were more than a year late and were never finally delivered by the time this project had finished.

We are not sure that the programme manager could have resolved the above issues, but he may have been able to influence at least one of them.

## 15. Future Work

Given that the ultimate aim of this project was not achieved i.e. to have VOMS-PERMISS-GT/OMII pilot services at the NGS, then further work is still required to do this.

The NGS has GT2 requirements and this project delivered GT4 OMII components. The NGS did take and does have a working PERMISS instance in relation to the SARoNGS infrastructure. The key bits still missing from this are some of the documentation.

## Appendix A. Related publications that build upon the VPman project

J. Watt, R.O. Sinnott, J. Jiang, G. Stewart, A. Stell, D. Martin, T. Doherty *Federated Authentication and Authorisation for e-Science*, in Proceedings of APAC 2007 conference, Perth, Australia, September 2007.

J. Watt, R.O. Sinnott, T. Doherty, J. Jiang, *Portal-based Access to Advanced Security Infrastructures*, UK e-Science All Hands Meeting conference, Edinburgh, September 2008.

R.O. Sinnott, T. Doherty, D. Martin, C. Millar, G. Stewart, J. Watt, *Supporting Security-oriented Collaborative nanoCMOS Electronics e-Research*, International Conference on Computational Science, Krakow, Poland, June 2008.

R.O. Sinnott, C. Bayliss, D. Chadwick, T. Doherty, B. Harbulot, M. Jones, D. Martin, C. Millar, G. Roy, S. Roy, G. Stewart, L. Su, J. Watt, A. Asenov, *Scalable, Security-oriented Solutions for nanoCMOS Electronics*, UK e-Science All Hands Meeting conference, Edinburgh, September 2008.

Non-conference paper talks and invited talks given related to VPman work include:

R.O. Sinnott, *Supporting Life Science Research through Shibboleth and Community Grid Portals*, demonstration and presentation given at HealthGrid 2007 conference, Geneva, Switzerland, April 2007.

R.O. Sinnott, *Experiences Developing e-Infrastructures across Biomedical Repositories at NeSC*, presentation given at EU workshop on Towards a European e-Infrastructure for e-Science Digital Repositories, Brussels, Belgium, March 2007.

R.O. Sinnott, *The UK e-Science Environment*, presentation given at UK-Malaysian e-Research workshop organised by UK High Commission, Kuala Lumpur, Malaysia, June 2007.

R.O. Sinnott, *Inter-disciplinary Research at Glasgow*, University of Glasgow, October 2007.

R.O. Sinnott, *To the Power of "e-"*, invited talk at Computer Science Meets Systems Science Workshop, Glasgow Caledonian University, November 2007.

R.O. Sinnott, *e-Science and the NHS*, talk given at NHS-HE Forum, University of Edinburgh, November 2007.

R.O. Sinnott, *Secure Data Integration*, invited talk given at National Cancer Research Institute, Wellcome Trust workshop, London, January 2008.

R.O. Sinnott, *Security and Geospatial Systems*, talk given at EDINA workshop, Edinburgh, April 2008.

R.O. Sinnott, *Usability and Interoperability for Grid Security*, invited talk given Trust and Security Workshop, Oxford, May 2008.

R.O. Sinnott, *BioGrids and Beyond*, invited talk at the International HealthGrid 2008 conference, Chicago, USA, June 2008.

R.O. Sinnott, *Lessons Learned in Developing and Supporting e-Biomedical Research*, invited talk given at Workshop on Building the e-Library, the University Health and Medical Librarians Group, Kelvin Conference Centre, Glasgow, Scotland, June 2008.

R.O. Sinnott, *e-Infrastructures for Inter-disciplinary Research across the Social, Clinical and Geospatial Domains*, CESSDA-PPP Workshop: How the CESSDA Infrastructure can utilise Grid technologies and e-social science methodologies to provide pan-European services, Manchester Conference centre, June 2008.

R.O. Sinnott, *The digital infrastructure security perspective: a brief overview of current and anticipated developments in e-Infrastructure security*, National Centre for e-Social Science workshop on Secure Access to Confidential Data, Manchester, UK, June 2008.

R.O. Sinnott, *Access, Use and Re-Use*, presented at Data Curation Centre (DCC-101) training course, Edinburgh, UK, October 2008.

R.O. Sinnott, *e-Infrastructure Security and Data Archives*, Invited Talk to UK Data Archives, University of Essex at Colchester, UK, November 2008.

R.O. Sinnott, *Requirements for Repository Environments: Supporting User and Provider Friendly Single Sign-On Models*, Invited Talk to Repository Curation Service Environments (RECURSE) Workshop at the Digital Curation Conference (DCC), Edinburgh, UK, December, 2008.

R.O. Sinnott, *VPman and SPAM-GP (the Directors Cut)*, Invited Talk at Security-workshop, Daresbury, UK, December, 2008.