JISC Final Report

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

Document Name			
Document Title	Final Report		
Reporting Period			
Author(s) & project role	David Chadwick (Project Director), Richard Sinnott (Glasgow PI), Andrew Richards (NGS Manager), Neil P Chue Hong (OMII-UK Director)		
Date	29 July 2009	**Filename**	VPManFinalReport.doc
URL	http://sec.cs.kent.ac.uk/vpman/VPManFinalReport.pdf		
Access	☐ Project and JISC internal		✓ General dissemination

Document History		
Version	**Date**	**Comments**
0.9	20 July	Final Draft for Review
1.0	29 July	Final Report (no changes made)

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

Table of Contents

Acknowledgements

This project was funded under the JISC e-Infrastructure Security programme. The direct partners in the project were:

The University of Kent (directly funded)
The National E-Science Centre at the University of Glasgow (directly funded)
The UK National Grid Service (self funded)
Open Middleware Infrastructure Institute (OMII-UK) (self funded)

The Universities of Manchester and Oxford, via the SARoNGS project, were also inter-related with the VPMan project as the outputs of both projects were inter-dependent. The London e-Science Centre (LeSC) was also involved as a subcontractor to OMII-UK. Finally Istituto Nazionale di Fisica Nucleare (INFN), Italy, was a key player as the VPMan and SARoNGS projects both depended on INFN developing a new VOMS attribute pull module.

Executive Summary

Both VOMS and PERMIS 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 together makes a more powerful solution for Grid security management than the sum of their parts. This purpose of the VPMan project was therefore to combine together VOMS and PERMIS for use in the UK National Grid Service. The specific objectives of the project were to:

- integrate VOMS and PERMIS, 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) 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 STFC (formerly CCLRC);
- distribute the integrated software as open source code.

The project achieved all its stated objectives apart from integrating the final software in an operational system at STFC. This was due to

a) the VPMan project running out of time before this final phase could be completed and
b) the SARoNGS project also running out of time so that integration of its code with the VPMan code could not be completed within the allotted time frame.

In addition to the stated objectives, the project also contributed towards the publication of four Open Grid Forum specifications [1-4] which specify protocol profiles for components of the grid authorisation infrastructure communicating with each other.

Whilst the software developed under the VPMan project by the University of Kent has been released as open source code to the public, some of the software that it uses, specifically from INFN, still has not been released as open source by its developers. Consequently a complete open source Grid authorisation system is still not obtainable.

At the start of the project VOMS only worked in attribute push mode, meaning that the user's VOMS attributes were pushed to GT4 along with the user's grid job. During the lifetime of the VPMan project, INFN produced a prototype VOMS pull mode service, allowing PERMIS to pull the user's attributes from VOMS. The INFN project had been due to finish more than a year before VPMan, but it still had not completed by the time VPMan finished. Consequently we never did manage to get open source code for the push service, and we had to rely on remote testing to a pilot push services run by INFN in Italy. Consequently VOMS in pull mode could never be tested in a fully integrated pilot project by NeSC. NeSC did manage to implement a direct call from an OMII-service to a VOMS server and pull the user's credentials from there to use in an authorisation decision. But this was implemented in the code itself and did not use PERMIS in pull mode.

PERMIS software relies on IAIK cryptography software from Austria which is not open source. The University of Kent has permission to release IAIK binaries integrated into PERMIS binary releases, but not IAIK open source as part of PERMIS open source releases. LeSC were commissioned by OMII to produce open source equivalents of IAIK for PERMIS, using Bouncy Castle software. They made the binary software available to Kent for testing, but not the source code. The code did not work correctly, but it was impossible to fix the problem without access to the source code, which LeSC did not provide until the end of project. By this time it was too late to fix the bug.

The project was large in terms of the number of partners (up to 8 organisations), and coordination was not always as smooth as one would have hoped for, especially when it was by email exchanges between developers. However, when the project partners met together for face to face meetings, good progress was usually made and any log jams were cleared. The project had its fair share of delays along the way, many of which had been anticipated in the risk analysis, including:

1. Experienced staff leaving which caused delays until new staff were recruited and trained.

2. The use of recently developed software, which was not fully documented, took much more time to build and learn to use than was planned.
3. The complexity of the combined solution is still non-trivial for many administrators – this includes the installation and configuration of VOMS as well as how to use VOMS attributes to make authorisation decisions with PERMIS. Whilst we have documented user guides on how to achieve this, it still remains non-trivial for many – hence our focus upon working directly with other projects to build demonstrators showing how these kinds of authorisation scenarios can be supported.
4. The non-availability of source code upon which the integrated solution depended. This significantly increased the time required for testing and debugging and led to many wasted man weeks of effort.

Background

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) 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 was planned to be integrated it into the National Grid Service (NGS) at STFC. However, its authorisation decision function is intentionally missing by design (in GT2, VOMS relies on some C modules known as LCAS). PERMIS on the other hand provides a feature rich, modular authorisation decision function, with a user friendly policy management interface, was already integrated into Shibboleth and GT4 at the start of the project, and was being integrated into the OMII-UK software environment as OMII-AuthZ by the London e-Science Centre (LeSC) during 2006. However, it has a less well developed privilege assignment function.

The VPMan project was designed to enhance the state of the art in several ways:

i) 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.
ii) Perform the integration in both GT4 and OMII-UK software
iii) Add support to PERMIS for the new VOMS attribute pull feature
iv) Contribute to and conform to the OGF authorisation standards

The above advancements are important since they will allow the NGS to run grid services whose authorisation functionality is provided by a policy based system rather than some fixed modules of C code (i.e. LCAS). Policy based authorisation systems provide a much finer granularity of control, as well as much more sophisticated rules such as separation of duties and break the glass policies. Conforming to OGF standards means that the authorisation components are swappable and alternative implementations can be used.

Aims and Objectives

The project objectives were 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 STFC;
- 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.

The project achieved all its stated objectives apart from integrating the final software in an operational system at STFC. Further work still needs to be done to achieve this.

Methodology

The overall approach was one of build-test-revise-test. The building was performed primarily by the University of Kent, along with the initial testing. The first set of user trials were performed by the University of Glasgow, NeSC, and any modifications as a result of these were made by the University of Kent. The final set of tests were expected to be carried out by the NGS, prior to mounting an operational service, but this part of the project could not be completed due to a lack of time.

The exact approach was actually more complicated than this, because the University of Kent had to integrate components from multiple providers as well as producing new code itself. Specifically, code was obtained from OMII-UK and GT4 for providing a basic grid service, replacement cryptography code for Bouncy Castle was provided by LeSC, and a test VOMS attribute pull service by INFN, Italy. Not all of these components were available at the same time, and when they were obtained not all of them would work correctly (see next section). In terms of interoperability between PERMIS and VOMS, the PI at Kent and the researcher from INFN (Valerio Venturi) were joint editors of the OGF draft which specified the protocol for pulling attributes from VOMS [1], so it was possible to ensure that both organisations conformed to the standard, as they were the authors of it. However, the standard did evolve during the lifetime of the project which necessitated some code changes by both parties, and the standard was not finalised until after the project had finished. Since we were never able to obtain source code from INFN in order to build and run our own VOMS attribute pull service we cannot be sure that the final VPMan implementation is fully conformant to the OGF standard or will interoperate in a bug free manner with the INFN code.

Implementation

The project had 8 participating organisations (2 directly funded by the project, 2 who were funding themselves, 2 who were funded by a different JISC sister project, 1 who was a subcontractor to one of the unfunded partners, and 1 who was funded in Italy). Consequently liaison and communication was more difficult than usual. Coordination was not always as smooth as one would have hoped for, especially when it was by email exchanges between developers. However, when the project partners and PIs met together for face to face meetings, good progress was usually made and any log jams were usually cleared.

The project was dogged by delays. It took OMII-UK and NGS longer than planned to provide use cases at the start of the project and when the NGS use case was provided it depended upon the output of the Shintau project (attribute aggregation) so had to be discounted. Then the RA at Kent left after only 6 months into the project and a replacement had to be recruited and trained, which caused a delay of some 4 months. But this paled into insignificance considering the VOMS pull software from INFN which was over 1 year late in providing a first working prototype and by the close of the project had still not delivered open source code that we could use for testing or building a real VOMS pull service. Furthermore when software from other partners was delivered to Kent it did not initially work as expected. OMII-UK, as part of another project, had already subcontracted LeSC to integrate PERMIS into OMII, however Kent were not involved in this project. This code was late in being delivered and was not well documented. After several months of trying and failing to get the new OMII-Authz PERMIS code to work at Kent, the problem was eventually tracked to the failure of OMII-UK's Tomcat to interwork with Sun latest Java version (1.5.0.10) which Kent was running at the time. The error did not manifest itself on the OMII-UK testbed using the same Java JDK version. However switching to an earlier version of Java at Kent fixed the problem, but only after causing further delays to the project. The Bouncy Castle interface code from LeSC, delivered as binary code, never did work correctly for signature verification. Many man weeks of effort were wasted by Kent trying to locate the fault, but because LeSC would not provide the source code to Kent, the problem was never fully

tracked down and fixed. Since the LeSC code was not released as open source code early enough in the project[1], it was not possible to switch PERMIS from IAIK binaries to Bouncy Castle open source code during the project. Use of IAIK does not prevent PERMIS from working, nor does use of IAIK with PERMIS interfere with the functioning of any demonstrators created for the VPMan project. However the use of IAIK libraries *does* limit the re-distribution of PERMIS source code and its embedding within derived works such as OMII-AuthZ because of the licensing conditions described later.

Despite these difficulties the NeSC at Glasgow undertook a variety of trials of the software that was produced throughout the project. The GT4-VOMS-PERMIS integration in push mode was applied in the MRC funded VOTES project for a data-oriented authorisation decision. In this case study, a VOMS server was used to host a *VOTES-diabetes* trial virtual organisation at NeSC Glasgow. Roles of *VOTES-doctor* and *VOTES-nurse* were supported in this VO. Through exploiting the VOMS graphical user interface Acacia software, users could create X509 credentials with embedded VOMS credentials which were pushed to a PERMIS protected GT4 service. This service supported a variety of methods each of which required particular VOMS attributes to access and use. It was demonstrated how different VOMS roles in push mode could be used to gain access to restricted methods – thus showing that the integration of VOMS-PERMIS and GT4 could successfully work in push mode. This software was demonstrated at numerous conferences and workshops along with the technical configuration of the various components involved. Various papers were also produced describing this scenario and its associated benefits.

Whilst it was not possible to demonstrate the integrated OMII-VOMS-PERMIS scenario due to time limitations as described above and lack of software from partners, the NeSC at Glasgow implemented a scenario which showed how OMII and VOMS could be integrated directly. In this scenario, the EPSRC pilot project, Meeting the Design Challenges of nanoCMOS Electronics was chosen. Specifically, the scenario showed how compute-oriented authorisation decisions could be supported. In particular, a GridSAM instance was used as the basis for an authorisation decision, where different DRM Connectors were the focal point of the authorisation decision. The implementation of the demonstration was based upon using the X509 digital certificate and extracting the DN of the end user. Using this information, a direct connection to a VOMS server at NeSC was made and the VOMS credentials for that user returned. Based on the returned credentials, the GridSAM server submission system implemented a choice of which DRM Connector to use. Ideally of course, it should have been the PERMIS decision engine that pulled the credentials from VOMS and made the decision, but given that this software was delayed (for reasons given above), a demonstration of how pull modus operandi with a VOMS server should work, was all that could be achieved at NeSC. This demonstration was also demonstrated at various conferences and workshops.

After completion of these scenarios, the funding for the researcher involved at NeSC Glasgow ran out, and no further refinements to the scenarios were possible.

It is worth noting that a further scenario implemented at NeSC Glasgow was actually getting VOMS to work on a HPC cluster using LCMAPS/LCAS. This is non-trivial and has only recently been supported on the NGS.

In early 2006, prior even to the writing of the VPMan proposal, OMII-UK had commissioned the OMII-AuthZ service from LeSC as an initial reference implementation of the OGF AuthZ standard to offer per-service, per-operation authorisation for Web Services. This implementation used an embedded instance of OpenPERMIS as a decision engine. This was a natural implementation decision by LeSC because OpenPERMIS was an existing decision engine with an established user base.

During an intellectual property audit of an alpha release of OMII-AuthZ delivered to OMII-UK in late 2006, it was discovered that the IAIK cryptography libraries shipped with binary PERMIS were subject to licence conditions limiting the use and even the redistribution of those libraries. At that point OMII-UK was not aware that Kent was permitted to ship an embedded copy of the IAIK libraries within binary PERMIS but not within Open PERMIS – therefore each end user of Open PERMIS would have

[1] LeSC did finally release the open source code to OMII-UK in November 2008, and this fact was relayed to Kent by OMII-UK in December 2008.

to obtain the IAIK binaries or source code from the suppliers and agree to non-commercial or academic use and to a no-export policy.

Discussions between Steven Newhouse, the then Director of OMII-UK and David Chadwick led to the idea that OMII-UK would attempt to fix the problem by replacing the IAIK library with a true Open Source equivalent. This software is the BouncyCastle cryptography library whose licence contains no restriction on use or redistribution. OMII-UK and LeSC worked on this within the OMII-AuthZ project and it was this work that was taken forward into VPMan in 2007.

The first cycle of development was carried out during VPMan prior to May 2007. At a meeting in May 2007 between staff from Kent, LeSC, and OMII-UK it was agreed that the LeSC implementation (PERMIS plus LeSC interceptor code plus BouncyCastle) would be verified by Kent using the PERMIS test suite. An initial pass through revealed several areas of failure but not too many to be discouraging. However this part of the project stalled at this point due to two reasons.

Firstly, the LeSC developer became unavailable for several months due to a family bereavement followed by a lengthy series of conference commitments.

Secondly, the IAIK library suppliers issued a new 'Open Licence' that relaxed the rights to re-distribute the runtime cryptography libraries so it was necessary to re-evaluate our assumptions. The new licence conditions were quite subtle:

1) Anyone could redistribute IAIK libraries in an Open Source software project provided that said software was licensed under GPL 2.0 with a restriction that the software was for academic or non-commercial use only.
2) Open Source suppliers wishing to use a licence other than GPL 2.0 could ask IAIK for a concession to approve a different Open Source Licence.

It was OMII-UK's initial opinion that the new licence gave Kent enough rights to re-distribute IAIK libraries freely within OpenPERMIS for academic or non-commercial use because Kent had obtained the concession referred to in '2)' above. However the new licence did not grant OMII-UK (or anyone else) sufficient re-distribution rights to make OMII-AuthZ a truly Open Source offering. Because OMII-UK's preferred licence is BSD like, OMII-UK would have had to obtain their own concession from IAIK and then they were unsure as to the rights of any downstream user to add OMII-AuthZ to any derived product. It was also questioned as to whether condition '1)' was even valid – there was a school of thought that said that "GPL plus conditions is not GPL".

Advice from OSS-Watch was sought and they concurred that the new licence was still too limiting to allow redistribution of PERMIS within derived works such as OMII-AuthZ. OSS-Watch also added that the restrictive nature of the IAIK licence was probably due to the presence of patented algorithms within the library, particularly the IDEA algorithm. IDEA is free for academic / non-commercial use but other use requires a licence from the patent holder (see http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm). It seems likely that IAIK's licence conditions are to protect them from possible liability of downstream users violating the IDEA patent. Interestingly, the BouncyCastle library also contains an implementation of IDEA, but their solution is to point out the patent in documentation and to permit any downstream use at the user's risk, placing the liability for compliance with the user.

None of these legal issues prevented the construction of functioning demonstrators within the VPMan project, providing that IAIK software and not Bouncy Castle was used. However it would possibly have prevented the deployment of PERMIS within OMII-AuthZ as production services on the NGS resources or campus facilities.

After determining that the revised IAIK license conditions did not satisfy their requirements, OMII-UK attempted to continue with the BouncyCastle replacement during the period that Kent's RA/Project manager was being replaced. Although some progress was made there were still two outstanding test suite failures that could not be resolved by either LeSC or Kent on their own. With hindsight, we see that the interaction between the LeSC and Kent research staff broke down at this point as neither party could pinpoint the problem on their own, and both had other tasks to work on. The problem was traced by Kent to a failure in LeSC's signature verification interface code, but without access to

LeSC's source code, it was impossible to pinpoint or fix the problem. Again with hindsight, OMII-UK should have pressed LeSC more strongly to release their source code to Kent, since although it was promised by LeSC on several occasions, it was never actually forthcoming.

Late in 2008, technical meetings were organised by OMII-UK between a specialist from Kent and LeSC. In keeping with the rest of the project, this face to face meeting produced a lot of positive agreement and resolved one of the outstanding two problems. The final bug has never been resolved, in part due to the disagreements about access to the LeSC source code already described.

Outputs and Results

The various trials and demonstrations of the software were documented in conference papers and at workshops. These included international conferences such as the Open Grid Forum (OGF22) meeting held in Cambridge, USA in February 2008; the IEEE International Symposium on Cluster Computing and the Grid (CCGrid 2008; the IEEE International Symposium on Parallel and Distributed Processing Systems with Applications, Sydney Australia, December 2008. Further demonstrations of VPman were also given at the UK e-Science All Hands Meeting in Edinburgh, September 2008 (including the GT4-VOMS-PERMIS and an OMII-UK-VOMS scenario in the nanoCMOS domain), and again at a UK e-Science Security Workshop held in Daresbury in December 2008.

OMII-AuthZ 1.0.0 is downloadable in source code form from the OMII-UK website. The default configuration is to install the embedded PERMIS instance to use the LeSC BouncyCastle code with the BouncyCastle cryptography library. However, the signature verification bug referenced elsewhere is still present so the implementation is not reliable. In principle OMII-AuthZ can be used with other OMII-UK services to protect operations, however OMII-UK cannot recommend it for production use at this time until the outstanding bug in the BouncyCastle interceptor code is fixed.

The PERMIS/VOMS/GT4 code is available for download as binary code from Kent's website, and this includes IAIK's cryptography library. There are no known issues with this code. Source code is also available from Kent without any cryptographic source code. In both case users still have to obtain the GT4 code from Globus and VOMS code from INFN, in order to build a complete system.

One indirect output of the project is four Open Grid Forum protocol specifications for the interactions of the various components of a grid authorisation infrastructure [1-4]. This has ensured that the project's outputs are conformant to Grid standards and will ensure inter-working with other authorisation products that may be developed in the future by other research groups.

Outcomes and Impact

Notwithstanding the countless delays described in the previous section, thanks to JISC giving the project two no-cost time extensions, the project was eventually able to deliver all of its original objectives except one, which was having a running operational service of GT4-VOMS-PERMIS or OMII-UK-VOMS-PERMIS at the NGS.

Below we go through the original objectives one by one and enumerate our achievements.

The project objectives were to:

- *integrate VOMS and PERMIS, more specifically the VOMS user management and attribute assignment function with the PERMIS policy based authorisation decision function;*

PERMIS has been enhanced in a number of ways. Firstly it is now capable of contacting a remote VOMS attribute authority and pulling the attributes from there as SAML assertions. Secondly it is possible to configure the PERMIS Credential Validation Service (CVS) with rules about which VOMS servers to trust to issue which attributes and have the CVS parse and validate the credentials that are obtained from there as either X.509 attribute certificates or SAML attribute assertions. Thirdly it is possible to configure obligations into PERMIS policies that allow user jobs to be run under specific user IDs or GUIDs according to administrator defined rules. Finally, it is now possible to trust an authority with any name that is subordinate to a configured name. The net result of this integration

work is that the NGS should now be capable of offering a service based on VOMS and PERMIS which offers an improved fine grained access control mechanism to grid applications, allowing them to run grid jobs that otherwise might not have been possible due to the limits in the existing security mechanisms.

- *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;*

The project produced two main software outputs, namely the integration of PERMIS and VOMS with GT4, and with OMII-UK. This integration allows an administrator to manage the users' attributes with a VOMS server, and to grant permissions to the attributes with PERMIS. The retrieval of the attributes is done by either push or pull mode. In the push mode, the user gives (pushes) his attributes (as digitally signed attribute certificates) to the Grid service, which are validated by PERMIS. In the pull mode, the user merely proves his identity to the Grid Service and then PERMIS pulls the attributes of the user from a VOMS server using a SAML attribute assertion. The integration of PERMIS with Shibboleth was already available prior to the start of this project and the integration of Shibboleth with Grid software and PERMIS was carried out by the Universities of Manchester and Oxford under the SARoNGS project. Appendix 1 provides a brief summary of their achievements by the end of that project.

- *validate the results in several representative major pilot applications run by the NeSC;*

The integration was validated at the NeSC in the following projects: the MRC funded VOTES project and the EPSRC nanoCMOS project. .We note that the results of VPMan have also guided work on a range of other NeSC Glasgow projects including the recently funded ENROLLER project; the ESRC funded DAMES project; the Wellcome Trust, EPSRC, ESRC, MRC funded SHIP project amongst others.

- *evaluate the combined software from user, administrator and Grid developer perspectives;*

From the end user perspective, the use of the integrated software demonstrated was based primarily upon the user interface given by the VOMS graphical user interface software, Acacia. It was this software where the users could assert which roles they wished to push to gain access to a particular remote service. From an administrator and Grid developer perspective, the integration of VOMS, PERMIS and flavours of Grid middleware remains a challenge and further work is required to make this easier to support and maintain. To this end, a major grant proposal has been submitted by NeSC and Kent to EPSRC to establish a National Centre for e-Security – submitted as part of the EPSRC Software Sustainability call[2].

- *integrate the combined infrastructure with the National Grid Service (NGS) at STFC;*

Within the NGS the outputs from the VPMan project are being taken for use in relation to the SARoNGS (Shibboleth Access to Resources on the NGS) project. It was envisaged that the PERMIS engine from the VPMan project would be coupled with the VOMS authentication work that is part of SARoNGS. At the end of the SARoNGS project, which is now in pre-production testing, the PERMIS engine was deployed by the NGS based at Oxford. Full deployment and integration of the PERMIS components is still pending further deployment work by NGS Operations.

- *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.*

The PERMIS/GT4/VOMS software is available in both binary and source code versions. The binary code is available from here:

http://sec.cs.kent.ac.uk/permis/integrationProjects/GT.shtml

and the new documentation is available from here:

[2] Unfortunately we recently found out that this will not be funded by EPSRC.

http://sec.cs.kent.ac.uk/permis/documents/PERMIS_Authorization_in_GT4.pdf

The open source software is available from

http://www.openpermis.org

The OMII-AuthZ source code is available from

http://www.omii.ac.uk/wiki/Downloads

Conclusions & Recommendations

Notwithstanding the large delays, the project has been about 80% successful. All of the objectives, except running an operational Grid service at the NGS, have been completed. However, there are a still a number of loose ends that need to be tidied up. These include:

1) obtaining the INFN VOMS SAML attribute authority code from Italy as open source
2) removing the known signature verification bug from LeSC/Bouncy Castle and making sure that the combined VOMS-PERMIS-OMII-UK/GT4 open source works together in a bug free manner
3) obtaining operational experience of running VOMS in pull mode using the VOMS SAML AA.
4) Integrating the VPMan code with the SARoNGS code to provide an operational service at the NGS

The following recommendations are made:

i) It is not best practise to have a project partner who is not directly funded by the project and who is not strongly dependent upon the project's outputs, since their commitment to the project is bound to be somewhat less than those of the partners who are directly funded by the project.

ii) It is not sensible or good practise to subcontract development work of a package to a third party who knows nothing about that package, without involving the authors/developers of that package, especially when the authors/developers of that package are involved in a related project which depends upon this subcontracted work. One must ask the obvious question "why were the authors/developers of the package not directly involved in the subcontracted work?" On the other hand it is not always possible to subcontract all work to the original authors/developers as this does not scale. But it is sensible for the authors/developers to have involvement of some kind to allow for cohesion across all work strands.

iii) It is imperative that a contribution process and policy is agreed between all organisations and any sub-contractors on an open source project at the start of the project, as simply licensing code under an Open Source license is not always sufficient to resolve all potential attribution and IPR conflicts.

iv) If projects are dependent upon software being developed by third parties, especially ones from overseas, then this is a high risk strategy for any project and there should be plenty of contingency built in to mitigate any delays that might arise from this.

v) Any project which is planning to provide new services or functionality to the NGS should be managed and run by the NGS (ie. the NGS should be funded by JISC to subcontract to other parties rather than the other parties being funded directly by JISC). It is not effective to have another party trying to manage such a project as they do not have the leverage or operational experience to try to direct how the NGS should pilot the new services. Furthermore if the other party does not provide the service that the NGS has contracted for, then the NGS can withhold payment to that party until the service is provided

Implications for the future

In order to fully capitalise on the extensive work carried out under the VPMan project, some additional de-bugging, integration and implementation work is still required by the various parties as mentioned above. OMII-UK/Kent/LeSC need to fix the remaining bug in utilising Bouncy Castle in PERMIS. We need access to the INFN's VOMS pull software in order to fully validate its integration. No operational experience has been gained by the NGS so far. No usability trials of an integrated pull mode have been run so far. We therefore do not know what additional features end users and administrators will actually require before an operational service can be fully functional and easy to use by the NGS.

In terms of sustainability of the PERMIS software, we are in good health. The Swiss Ministry of Defence is currently hardening the PERMIS suite of software. They are investing many hundreds of thousands of Swiss Francs in this and have several commercial software engineers working full time on re-engineering the PERMIS code so that it is suitable for military grade use. The first fruits are now available to the public from the EC OSOR web site (www.osor.eu) where the hardened PERMIS software is being published. The SWISS MOD are using PERMIS for an Air Force application since in their words it is the only fully secure RBAC based system in town. They are donating all the hardened code back to the University of Kent and we plan to base all our future developments on this code base once the hardening is finished. The University of Kent is currently a partner in a large EC FW7 Integrated Project called TAS3, which is providing funding of nearly €1M to Kent to continue to develop the PERMIS software suite. In the TAS3 project we are adding support for yet more[3] sophisticated authorisation policies such as Break the Glass [5], and multiple policy evaluation via a Master PDP, which will provide conflict resolution of the decisions returned by the subordinate PDPs. This will allow multiple stakeholders to write their own policies independently of each other. This becomes important once we have privacy policies that require user consent. The user will be able to provide his own sticky policy for his personal data, and have this evaluated by one of the subordinate PDPs. Legal constraints and organisational policies can also be part of the mix that has to be evaluated by the Master PDP.

OMII-UK have taken over as custodians of the OMII-AuthZ code base and have been assessing the options for taking it forward with greater community participation; different scenarios have been proposed for its use. OMII-UK will continue to work with PERMIS, VOMS and Shibboleth as the NGS and UK institutions move forward in their requirements for securing services.

References

[1] V. Venturi, T. Scavo, D.W. Chadwick, "Use of SAML to retrieve Authorization Credentials", OGF GWD-R-P, 25 June 2009
[2] David Chadwick, Linying Su. "Use of WS-TRUST and SAML to access a Credential Validation Service". OGF GWD-R-P, 25 June 2009
[3] David Chadwick, Linying Su, Romain Laborde. "Use of XACML Request Context to access a PDP", OGF GWD-R-P, 25 June 2009
[4] David Chadwick. "Functional Components of Grid Service Provider Authorisation Service Middleware", OGF GWD-I, 25 June 2009.
[5] Ferreira A, Cruz-Correia R, Antunes L, Farinha P, Oliveira-Palhares E, Chadwick D W, Costa-Pereira A. "How to break access control in a controlled manner". In CBMS 2006, Proceedings of the 19th IEEE International Symposium on Computer-Based Medical Systems, Salt Lake City, Utah, 22-23 June, 2006, pp847-851

Appendix 1. Brief report of SARoNGS Project

Andrew Richards reported the following to VPMan on 14 April 2009

The current situation is that the SARoNGS project is now officially finished and we are in the process of writing the final report. The service is now the responsibility of the NGS though due to technical

[3] PERMIS already supports sophisticated policies such as Separation of Duties, Coordinated Access Control, Delegation of Authority and Attribute Aggregation, as well as standard and hierarchical RBAC.

issues in joining the Access Management Federation, specifically with metadata, the service is not yet in full production.

As for the PERMIS integration, this work was done mainly at Oxford and completed to the best it could, pending deployment as a full service as part of SARoNGS. Due to the ongoing technical issues with the SARoNGS core service, the PERMIS components were not classed as required at initial deployment. It is my current understanding that the developed work from Oxford has been delivered to STFC and will be deployed once the core SARoNGs framework is working and that in general PERMIS-SARoNGS integration has been achieved.

Tiejun Ma from Oxford added the following later on the same day

We use the PERMIS decision engine as a Web service in the Apache Tomcat with gLite enabled e-Science certificate security authentication protection. Within our scope of work, the CTS will be the only Web service client, which is enabled for access the PERMIS Web service decision engine. SAML 2.0 and XACML 1.0 are used as the communication protocols between the CTS and the PERMIS. The decision request will contain user's DN with all attributes, target DN and request actions. CTS will decide whether to create VOMS credential based on the actions. We adopted the UK federation metadata (stored in LDAP as permis policies) as the allowed institutes specification file for designing the authorization policy, so that all the institutes and their members within the UK federation will be recognized by our policy. The allowed VOMS roles and groups for each Shibboleth eduPersonSopedAffiliation value are stored as obligations in the policy. In order to keep consistency with the federation specification, we have designed a policy generator, which will check the newest published UK federation metadata then automatically update the policy stored within the policy repository to avoid false denial of accessing the UK National Grid Service (Robert implemented a policy generator running on the CTS server to translate the UK federation metadata into permis policies and store it in the LDAP).

At the moment, the permis web service and the policy repository is running at Oxford as a test server, we have tested it against the CTS's authorization request and it works. That is what we achieved so far. But it is not fully deployed as a production server as a NGS service yet. Hopefully, this information can help.