



JISC Project Plan

Project Information			
Project Acronym	SARoNGS		
Project Title	Shibboleth Access to Resources on the NGS		
Start Date	January 2008	End Date	January 2009
Lead Institution	STFC		
Project Director	Dr Andrew Richards		
Project Manager & contact details	Dr Andrew Richards STFC e-Science Centre Rutherford Appleton Laboratory Harwell Science and Innovation Campus Chilton Didcot Oxfordshire Ox11 0QX		
Partner Institutions	STFC (Rutherford Appleton Laboratory), University of Oxford, University of Manchester		
Project Web URL			
Programme Name (and number)	e-Infrastructure		
Programme Manager	James Farnhill		

Document Name			
Document Title	<i>Project Plan</i>		
Reporting Period			
Author(s) & project role	Andrew Richards (PI), Jens Jensen (CI), David Wallom (CI), Mike Jones (CI)		
Date	12/02/2008	Filename	SARoNGS_ProjectPlan (8.2).doc
URL	<i>if document is posted on project web site</i>		
Access	<input checked="" type="checkbox"/> Project and JISC internal	<input type="checkbox"/> General dissemination	

Document History		
Version	Date	Comments
8.1	30/01/2008	Final Version to JISC (formatted in project template, sequentially numbered to follow on from project proposal documents)
8.2	12/02/2008	Final version to JISC (Updated coversheet and IPR statement)

Overview of Project

1. Background

Building on the work of the SHEBANGS and ShibGrid projects it is proposed to take the outputs from both these demonstrator projects and provide a production ready service for the NGS. To achieve this aim, existing Shibboleth work from the GEMS projects will be integrated as part of the development, in order to provide real world examples of where the shibboleth authentication model can be used and integrated with a production grid service. This will also provide production ready models applicable to other resource providers such as VRE's and institutional repositories.

The ShibGrid project has developed a prototype to enable NGS users with or without UK e-Science certificates to securely access those resources, through the integration of Shibboleth, GSI (Grid Security Infrastructure) and MyProxy. This aimed to bring the confidentiality and privacy aspects of shibboleth to both grid users and service providers, while making the tools as easy as possible to use. Users are able to access internal and external recourses seamlessly using a single institutionally controlled identity.

The SHEBANGS projects aims were divided loosely into three parts, the first part of the project focussed on the development of the basic *Credential Translation Service* (CTS). This CTS creates GSI credentials which are then delegated to a trusted MyProxy server for the consumption by a portal. The second part incorporates VOMS (Virtual Organization Membership Service) assertions created at the CTS into these GSI credentials. The third part incorporates Identity providers from the FAME-Permis project (x) and MIMAS SHIMMER (x) project.

2. Aims and Objectives

In this project it is proposed to take the first two components from SHEBANGS and deliver a production quality service for use by NGS users and resource providers. The project will deliver a standard platform for integrating external resource providers into the NGS using Shibboleth authentication mechanisms. This will be in the form of a production quality CTS service, developed to work with standard VOMS services and provisioned with web service interfaces such that external resource providers can interface with the NGS with minimal development effort required. At the Shibboleth authentication level the service delivered as part of this project will interface with the UK Access Management Federation and thus provide a transparent and seamless access to grid resources for users who already have access to a Shibboleth identity.

It is also proposed that the project tracks the work of the VPMAN project, currently in progress and led by Prof. David Chadwick, of the University of Kent, with whom the NGS is participating. It is seen as essential for the NGS that this occurs in order to minimise overlap in development effort and to achieve integration of an authentication and authorisation platform for access to NGS resources. The VPMAN project has the potential to provide a resource provider with the ability to set access policies for different roles as defined in the NGS VO's.

To facilitate deployment of these technologies the GEMS project, representing the interests of MIMAS, will be enabled during the 12 month period of this project but it is expected that the work will facilitate the future integration of other service providers such as institutional repositories, VRE's and data sets provisioned by other providers such as EDINA.

3. Overall Approach

The project has been divided into 7 work packages, each is described below. The Gantt chart indicates the timing of the work package implementations.

Work Package	Jan 2008	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec 2008
1												
2												
3												
4												
5												
6												
7												

Work Package Key:

WP1: Management

WP2: Shibboleth based Certificate Authority

WP3: Shibboleth based VOMS Front-end

WP4: VO Registration Interface

WP5: CTS based Virtual Organisations

WP6: Developing VOMS-aware services

WP7: Future recommendations: Access Management Federation Scoping

4. Project Outputs

To summarise, the deliverables from this project are;

- Project management work plan and final report
- Interim requirements report after 2 months of project start, final report within 1 month of the end of the project
- A Modified Credential Translation Service (CTS) which works with the “Shibbolised” MyProxy
 - CTS to be enabled to speak the “Shibbolised” MyProxy protocol.
 - CTS to present user interface (VO registration and Credential Management interface).
 - Incorporation of PERMIS into CTS (to allow the VO which hosts the CTS to create policy based decisions for credential release).
 - CTS to provide database to store user preferences
 - CTS to provide WS interface
- A modified MyProxy Server
 - Accepts password change mechanisms based upon SAML assertion authentication.
- One instance of CTS registered as an SP in the UK Federation, to permit every user from every institution with an IdP access to the NGS.
- Software, including various integrated upload and download tools supporting non-portal access.

- Secure website service for use with Shibboleth (to host the CTS).
- Production Deployment of PERMIS from the VPMAN project.
- Exemplar service for accessing MIMAS data sets hosted on NGS Production hardware.
- Project website, documentation and international workshop on usage of VO enabled Shibboleth within a grid environment.
- Outputs submitted to e-Framework.

5. Project Outcomes

Contributions to the JISC e-Framework

Many of the JISC e-Infrastructure projects are currently either using the current PKI system which some users find difficult and cumbersome or bespoke solutions developed on a per project basis.

This project will contribute a common platform for authentication and authorisation, by building on the existing shibboleth work of the ShibGrid and SHEBANGS projects for authentication and work to integrate with the VPMAN project for authorisation.

To the e-Framework this project will contribute:

- A common security and authorisation platform that can easily be adopted by other service providers across the local, national and international grid infrastructures. Individual components will be contributed as SERVICES to e-Frameworks.
- Extend the UK Access Management Federation to enable users to access grid enabled resources. For example, enable access to existing services such as MIMAS. Contribution to e-Framework SUMS as use cases on integrating MIMAS and reference documentation provided under the e-Framework GUIDES.
- Recommendations on attribute requirements for the UK Access Management Federation, in order to fully support grid infrastructures. This will be as a contribution to e-Framework GUIDES.

6. Stakeholder Analysis

Stakeholder	Interest / stake	Importance
NGS	Using the project's outputs in their service	Very high
OMII	Using the project's outputs in their open source software	High
VOMS development team	Ensuring their interfaces and specifications are usable by others	Medium
STFC	Associate developers	Very High
University of Oxford	Associate developers	Very High
University of Manchester	Associate developers	Very High
MIMAS	Developer/consumer	Medium
JISC	Funding Body	Medium

7. Risk Analysis

Key for risk analysis.

Strategy	
Acceptance	Can live with it - avoidance/mitigation more costly than impact
Avoidance	Take steps to prevent risk from occurring
Mitigation	Take steps to lessen the impact of the risk, should it occur.
Transferral	Pass the risk onto another system.
Contingency	Needs alternative plan of action if risk materialises

Project Acronym: SARoNGS
Version: 8 (FINAL)
Contact: Dr Andrew Richards (STFC)
Date: 30/01/08

Area	Owner	WPID	Description	Impact	LIKELIHOOD (1-4)		Risk	Strategy	Action to avoid/mitigate	Timescale	Urgency	
					LI	IM						
Staff	AR	1	1	Difficulty hiring - not enough effort to complete tasks on time	Some goals delayed or cannot be met	2	3	6	Mitigation	Hire contractors. Temporarily reassign other people	Project	High
Staff	AR	1	2	Staff retention - losing knowledge/skills means goals can't be met	Some goals delayed or cannot be met	3	3	9	Mitigation	Document technical issues, share skills in int'l works	Project	High
UKFED	JJ	3	3	CTS not accepted by UK Federation	Lose UK Fed institutions as IdP	1	4	4	Avoidance	Use UKFed SP requirements in design. Review	Far	Med
NGS	MJ	3	4	VOMS server will need modifications	Cannot deploy in NGS (must use NGS VOMS)	1	3	3	Avoidance	Manage user req/expectations. Work with VOMS developers if necessary	Med	Low
NGS	AR	2	5	MyProxy CA not trusted by NGS	Cannot run jobs on NGS	1	4	4	Avoidance	Build on best practices for SLCS. Use key token.	Far	Low
UKFED	AR	3	6	UK Fed does not permit enough IdP attrs to meet user req.	Weakens impact of VO mgmt - less trust in user provided attrs	2	3	6	Mitigation	Can keep int'l attrs in CTS user and VO databases	Med	Med
UKFED	AR	3.5	7	Won't meet VO use cases because of UK Fed rules disallowing attr passing	Weakens impact of VO mgmt - less trust in user provided attrs	2	2	4	Mitigation	Keep dialogue with VOs. Implement conversion scheme - needs investigating	Near	Med
NGS	AR	1	8	NGS users will not use the system	Less practical impact, not broadening NGS user base	2	3	6	Avoidance	Encourage uptake with easier authentication, fit into existing NGS ecosystem. Focus on usability. Get early testing and feedback. Consider NeSC training.	Far	Med
Ext'l	AR	All	9	Hardware procurement/testing/acceptance delays project	Project delayed	2	3	6	Avoidance	Spec hardware early. Piggyback on NGS sites' procurement and acceptance procedures	Now	Med
Req	AR	All	10	Hardware underprovisioned	Cannot run satisfactorily in prod'n	1	2	2	Avoidance	Spec hardware early - build on experience from ShibGrid and SHEBANGS	Now	Med
Tech	AR	2	11	MyProxy CA needs modifications	Cannot interface to std MyProxy	2	3	6	Mitigation	Run own MyProxy server (cf ShibGrid)	Med	Med
User	AR	1	12	Conflicting requirements from users (e.g. re VO mgmt)	Cannot meet user requirements	3	2	6	Avoidance	Early requirements capture. Nominate user group.	Near	Med
User	AR	1	13	User requirements imprecise or incomplete, or they change their minds	Time wasted on development	4	2	8	Avoidance	Hold user workshops/dialogue. Get early testers.	Med	Med
Ext'l	AR	2-7	14	Ext'l dependencies (eg libraries) licensing incompatible with proj sw licence	Cannot deliver complete sw package	3	2	6	Avoidance	Manage expectations and change	Med	Med
UKFED	AR	3	15	UK Federation switches software infrastructure or changes SP technical requirements (e.g attr push/pull)	Need to spend time to adapt the CTS SP	1	3	3	Acceptance	Negotiate with ext'l developers	Med	Med
Ext'l	AR	2-7	16	Infrastructure compromised (security incident)	Need to spend time fixing/tracking	2	3	6	Avoidance	Pick ext'l libraries with compatible licences (if avail)	Near	Med
Ext'l	AR	2-7	17	Support for ext'l dependency fails	Need to spend time finding replacement	2	3	6	Mitigation	Follow best practices for systems operations	Project	High
Plan	AR	1	18	Distributed development slows down development	Duplicate effort, or leaving gaps open	3	3	9	Avoidance	Can take over software (if permitted by licence) till replacement is found	Project	Low
Tech	AR	1	19	Released software not stable, or doesn't meet user requirements	Users will not use the system	1	3	3	Avoidance	Allocate tasks and responsibilities clearly to partners. Hold coordination meetings.	Project	Med
Plan	AR	1	20	System not picked up outside NGS	Less impact	3	1	3	Avoidance	Implement clear dev guidelines and release procedures. Get early user input.	Med	Med
Tech	AR	1	21	Unforeseen technical glitches cause delays	Project delayed, or need to drop some targets	3	3	9	Mitigation	Use NGS and JISC for dissemination and outreach, also other venues like other Shib federations	Far	Low
Plan	AR	1	22	Insufficient funding/effort for coordination or management	Project could go off target	2	3	6	Mitigation	Careful technical planning - build on existing expertise from SHEBANGS and ShibGrid. When possible and justified, have "Plan B"	Med	Med
Tech	AR	1	23	(New) developers need training/learning before working 100%	Project delays	3	3	9	Mitigation	Delegate more responsibilities	Project	Med
User	AR	1	24	Cannot meet all user requirements/expectations	Users disappointed, bad publicity	3	2	6	Avoidance	Avoid isolated developers. Have a developer workshop/technical coord meeting early	Now	High
Plan	AR	1	25	Need to hire contract staff to complete targets	Delays, possibly risking components not fitting well into remaining software	2	3	6	Mitigation	Allocate well defined tasks only to contractors	Med	Med
Plan	AR	1	26	CA not agreed before project starts	Possible delays, or later disagreements	4	1	4	Acceptance	We've worked together before, unlikely to have major issues	Now	Med
Plan	AR	1	27	Fundamental disagreement between project partners	Goals not met	1	4	4	Acceptance	We've worked together before, unlikely to have major issues	Project	Low
Ext'l	AR	1	28	NGS radically changes infrastructure, or disappears, etc. User account via portal and non-portal access not integrated - dual registration (mapping existing esc DN to ePTID) may not be technically feasible	Developed software which won't be used	1	4	4	Contingency	Release software to other shib communities - or EGEE?	Far	Low
Tech	AR	1	29	Insufficient effort to meet all project goals	Cannot deliver all promised targets	2	3	6	Mitigation	Manually map the affected users, probably via their email addresses. Requires building extra email confirmation.	Med	Med
Plan	AR	1	30	Insufficient effort to meet all project goals	Cannot deliver all promised targets	2	3	6	Mitigation	Prioritise goals. Liaise with stakeholders re priorities	Med	High
Plan	AR	1	31	Early completion - all goals met before end of project	Developers twiddling thumbs	1	1	1	Mitigation	Get developers to improve system - and documentation. Suggest additional tasks to be approved by stakeholders	Med	Low
Tech	AR	1	32	Proprietary components (eg HSM) become unsupported or unavailable or will not fit as planned into this project	Delays, or cannot meet specifications	2	2	4	Contingency	Find alternative solutions, possibly reducing security or performance	Med	Low
Tech	AR	1	33	Portal developments/code will not be used by existing portals (eg due to technical incompatibility with portal frameworks)	Users will have to use two different portals	3	3	9	Avoidance	Work closely with NGS portal developers. Use standards whenever possible.	Med	Med
User	AR	1	34	Users want non-portal access, or will not use portals for reasons not related to this project	Lessens impact of this work	2	2	4	Contingency	Test EGEE cmd line tools. Develop own interface to MyProxy, using CTS interface for acct mgmt	Med	Med
Plan	AR	1	35	STFC funding uncertainty causes problems	Can lose staff or difficulty hiring	2	3	6	Mitigation	Pass skills or work to other partners	Project	Med

8. Standards

Name of standard or specification	Version	Notes
X.509 proxy certificates	RFC 3820	Use as is
X.509 attribute certificates	X.509	Use VOMS variants
SAML (attribute assertions)	SAMLv1.1 or 2.0	Use to pull attributes from a VOMS server
XACML (request context)	V2	Use in GT4 to interface to PERMIS PDP

9. Technical Development

During development all software will be designed before code is written and reviewed by the project managers at each partner site. CVS versioning will be used to ensure the developers are using the most up to date code. Backups of the CVS server ensure that the development process will be protected against hardware failure. Also there will be developer guidance, and QA and release procedures

Any software delivered in this project will as far as we can be made available under an Open Source Initiative (OSI) approved Open Source licence. This might fail in dependence on external components with more restrictive licensing, where the timescales of this project do not permit us to develop an open source solution, nor to strengthen an existing one. In this case we will indicate this and suggest how to work around it.

10. Intellectual Property Rights

Under the Universities of Oxford and Manchester and STFC policies on intellectual property (which cover all employees and students), both institutions claim ownership of a range of intellectual property rights with commercial potential. The University does not assert any claim to the ownership of copyright in artistic works, books, articles or lectures, apart from those specifically commissioned by the University. Results arising from projects funded by the JISC at Oxford, Manchester and STFC would therefore usually be shared and owned in the first instance by the collaborating parties as the employing institutions. The University Of Oxford seeks to maximise the commercial potential of its intellectual property through its wholly owned technology transfer company, ISIS Innovation Ltd, the University of Manchester has similarly the University of Manchester Intellectual Property Limited (UMIP) and STFC will similarly seek to exploit developments through the CLIK technology transfer company.

Notwithstanding the above statement on IPR for the respective institutes involved in this project, the JISC has the license to perpetual use within the HE and FE sector.

Project Resources

11. Project Partners

The project partners are the STFC (Rutherford Appleton Laboratory), the University of Oxford and the University of Manchester, which encompasses the work of the MIMAS development as well.

There will be the equivalent of a full time developer at MIMAS - Manchester, NGS sites of Oxford and Manchester. At STFC-RAL, there will be 1.0 FTE in development effort. It is anticipated that the individuals listed in key personnel will play at least an advisory role in the project. At STFC-RAL 0.4FTE will be allocated to cover project management by Dr Claire Devereux and project direction by

Project Acronym: SARoNGS
Version: 8.1
Contact: Dr Andrew Richards
Date: 30/01/08

Dr Andrew Richards with Co-investigators Dr Mike Jones at Manchester and Dr David Wallom at Oxford.

It is planned that the Consortium Agreement will be signed by project partners before the end of January 2008. A draft copy of the CA has been circulated to all project partners.

The contact details for the project PI and CI are:

Dr Andrew Richards

STFC e-Science Centre
Rutherford Appleton Laboratory
Harwell Science and Innovation Campus
Chilton
Didcot
Oxfordshire
Ox11 0QX

Dr Jens Jensen

STFC e-Science Centre
Rutherford Appleton Laboratory
Harwell Science and Innovation Campus
Chilton
Didcot
Oxfordshire
Ox11 0QX

E-Mail: j.jensen@rl.ac.uk
Tel: 01235 446104
Fax: 01235 445945

Dr David Wallom

OeRC
c/o 13 Banbury Road
Oxford
OX2 6NN

E-Mail: david.wallom@oerc.ox.ac.uk
Tel: 01865 283378
Fax: 01865 283375

Dr Mike Jones

Research Computing Services
University of Manchester
Oxford Road
Manchester
M13 9PL

E-Mail: mike.jones@manchester.ac.uk
Tel: 0161 275 7038
Fax: 0161 275 0637

12. Project Management

The project will be led by the STFC, by Dr Andrew Richards. Project Coordination will be provided by Dr Claire Devereux.

Dissemination will occur throughout the project as well as within the specific work packages through a web site and attendance at appropriate JISC and e-Science meetings. The initial deployment will be done on test systems currently located at Manchester and Oxford. The NGS liaison officer, Dr Gillian Sinclair will be involved as part of her NGS role to coordinate dissemination activities. It is proposed to hold a workshop at NeSC at the end of the project.

Key members of the team are described below. The principal investigator **[PI]** and co-investigators **[CI]** are noted.

STFC

Dr Andrew Richards (STFC) [PI] is the Executive Director for the UK National Grid Service and head of the Grid Deployment Group within the STFC e-Science Department. He has worked within e-Science for over 5 years leading the development and deployment of grid infrastructure and advising on numerous grid projects, including ShibGrid and the current JSDL Applications Repository work.

Dr Jens Jensen (STFC) [CI], is the CA Manager of the UK e-Science Certification Authority (CA) and is responsible for its operation and policies. He represents the UK in international CA collaborations, works with other countries to join them into the Global Grid PKI, and negotiates trust for the UK with large resource providers. He currently leads Grid single sign-on effort within STFC, integrating the site Active Directory infrastructure with Grid interfaces for DIAMOND, STFC's ISIS neutron source, and laser facility – work which is relevant for this proposal. He is a member of the petabyte tape-store group at STFC and is also responsible for the deployment and support of Grid storage middleware to GridPP, the UK's particle physics grid. He has published papers on *inter alia*, certificate management, Grid security infrastructure, storage, Grid interfaces, software deployment, representation theory, and quantum cryptography.

Dr Claire Devereux (STFC) is the NGS and EGEE project support officer and will be providing project coordination and project management support for the SARoNGS project.

University of Oxford

Dr David Wallom [CI] is the Technical Manager of the Oxford e-Research Centre. In his present role he engages the wider community within the university with e-Science tools and technologies and especially with Oxford's e-Infrastructure including Campus grid, Virtual Research Environments and the institutional repository. He has advised the ShibGrid project on usage models within campus grids. He has a degree in Applied Physics from Coventry University with a year in industry and a PhD in Experimental Particle Physics from the University of Bristol. Currently he is chair of the UK e-Science Engineering Task Force and co-chair of the Production Grid Services Research Group of the Open Grid Forum (OGF).

Kang Tang has a Masters in Computer Science from UCL. He has worked as the ShibGrid developer at Oxford and has been key in the integration of Shibboleth with the NGS portal. During the ShibGrid project he has acquired substantial experience in the operation and usage of Shibboleth and its interactions with various JSR168-compliant portal frameworks.

University of Manchester

Dr Michael Jones [CI] specializes in Grid security, having worked on the JISC AAA projects A2Z [A2Z], Evaluation of the Community Authorization Server [CAS-eval], as well as the UK e-Science CA, the e-Social Science demonstrator project SAMD [SAMD] (where he developed a plug-in module to provide GSI support in a standard Apache Web server). He developed and delivered the security module of the Grid Support Centre's training course on Globus. He is currently responsible for the deployment and operation of VOMS for the NGS, and is the architect and lead developer of SHEBANGS. He represents ESNW on the UK Grid engineering Task Force, and operates the Manchester Registration Authority for the UK e-Science CA.

MIMAS

The person designated to work on this project at MIMAS is pending confirmation.

13. Programme Support

No specific requirements, though the project is happy for the programme manager to participate within the regular meetings.

14. Budget

The budget as agreed for the SARoNGS project is attached in Appendix A. There are no changes to the budget from the original proposal.

Detailed Project Planning

15. Workpackages

Appendix B contains the detailed descriptions of the 7 work packages for this project.

16. Evaluation Plan

Timing	Factor to Evaluate	Questions to Address	Method(s)	Measure of Success
	Access to NGS using Shibboleth ID	Can users access NGS resources using their local Shibboleth ID ?	Testing with user groups	>95% of user are able to achieve their objectives
	Software deliverables (formative)	Will the CTS software (including clients) allow Shibboleth users to access their resources?	Testing with user groups	>95% of user are able to achieve their objectives
	Pilot NGS service	Will the PERMIS-VOMS software improve the NGS?	Questionnaire	75% of users and administrators surveyed are satisfied or very satisfied with the new NGS access mechanism
Year after completion	Take up of open source software	Is there take up by the community at large?	Count number of downloads	200+ downloads in initial 12 months after release.

17. Quality Plan

Output	Quality criteria	QA method(s)	Evidence of compliance	Quality responsibilities	Quality tools (if applicable)
User Documentation	Fitness for purpose	Review and test by independent users	Test report	Project Manager	Word processor
Dissemination papers	Leading edge	Review by external reviewers	Accepted for conference or journal	Authors of paper	Word processor
Design documentation	Fit for purpose	Internal reviews	Signed off by Project Director	Project Director	Word processor, SVN
Software deliverables	Performs as expected	Code inspections	Integrated into NGS	Project Director	CVS, Regression test bench
Background info document	Comprehensive and clear	Review by project members	Accepted by project team for publication on project web site	Project Manager	Word processor
Use cases document	All possible configurations covered	Review by project members	Accepted by project team for publication on project web site	Project Manager	Word processor

18. Dissemination Plan

Timing	Dissemination Activity	Audience	Purpose	Key Message
	Web site	Global grid community	To raise awareness	Project objectives
	Newsletters, mailing lists, web sites about NGS service	UK grid community	Engage the community	New Shibboleth access to NGS is available
	Conference presentations	Conference attendees	To publicise the project and its results	A new security service is available
	Demonstrations	Conference/OGF/AHM /Workshop attendees	Promote the project	New service and software is available

19. Exit and Sustainability Plans

Project Outputs	Action for Take-up & Embedding	Action for Exit
Software deliverables and	1. NGS to incorporate software into	Access. Make software

associated documentation	their ongoing service.	available for download. Preservation. ?? Maintenance. IPR. None needed.
Case studies and best practice examples, a "How To" document	Widely disseminate these at various web sites	Access. Have available on various web sites for download Preservation. ?? Maintenance. IPR. Users should be given permission to copy for own use

Sustainable project outputs

Project Outputs	Why Sustainable	Scenarios for Taking Forward	Issues to Address
CTS	Standards based, open source application	Encourage open source community to build around it, expand to cover more than Shibboleth/Grid (PKI) interoperation.	How to fund, finding appropriate funding.

Appendixes

Appendix A. Project Budget

STFC	Jan-Mar	Apr-Dec	Total
Directly Incurred Staff Costs			
Staff total costs (A)	19454	60404	79857
Non-Staff at STFC			
Travel and expenses	1435	4305	5740
Hardware/software	1025	3075	4100
Dissemination		2138	2138
Total Non-Staff (B)	2460	9518	11978
Directly Incurred Total (A+B=C)	21914	69922	91835
Directly Allocated Estates (D)	3643	10946	14589
Indirect Costs (E)	19954	59960	79914
Total Project Cost STFC	45511	140828	186338
Manchester RCS and MIMAS			
Directly Incurred Staff Costs			
Staff total costs (A)	23058	69173	92231
Non-Staff at Manchester			
Travel and expenses	1470	4410	5880
Hardware/software	1050	3150	4200
Dissemination		2242	2252
Total Non-Staff (B)	2520	9802	12322
Directly Incurred Total (A+B=C)	25578	78975	104553
Directly Allocated Estates (D)	8338	25014	33352
Indirect Costs (E)	22764	68292	91056
Total Project Cost Manchester	56680	172231	228911
Oxford University			
Directly Incurred Staff Costs			
Staff total costs (A)	10473	31423	41896
Non-Staff at Oxford			
Travel and expenses	735	2200	2935
Hardware/software	550	1650	2000
Dissemination		1143	1143
Total Non-Staff (B)	1573	4720	6293
Directly Incurred Total (A+B=C)	12046	36143	48189
Directly Allocated Estates (D)	3082	9245	12327
Indirect Costs (E)	10803	32412	43215
Total Project Cost Oxford	25931	77569	103500
Total Project Cost	127787	390963	518749
Amount Requested from JISC	102229	312771	415000
Institutional Contribution from STFC	9102	28166	37268

Project Acronym: SARoNGS
Version: 8.1
Contact: Dr Andrew Richards
Date: 30/01/08

Institutional Contribution from Manchester	11336	34446	45782
Institutional Contribution from Oxford	5119	15581	20700

Appendix B. Workpackages

Work-package 1: Project Management

Description: Running throughout the project, this work-package aims to ensure the overall co-ordination of the project including the development of a detailed work-plan; to ensure adequate liaison and reporting between the project and stakeholders including funding bodies and information resource providers. This work-package will also manage the submission of outputs to the JISC e-Framework.

Deliverables: Project work plan, consortium agreement, overall project deliverables, completion report, e-Framework outputs, final report.

Work-Package 2: Shibboleth based Certificate Authority

Description: To enable individuals to make use of resources in a distributed environment it is vital to provide the individual with credentials from a trusted authority. Computational and data grids require X.509 based credentials from a national Certificate Authority.

The UK eScience certificate authority currently provides a Public Key Infrastructure based on in-person registration and user possession of long term private keys. This project aims to reduce the overhead by taking the ShibGrid MyProxy CA, deploying it in a limited production environment, and further developing it to incorporate hardware signing modules.

The ShibGrid MyProxy CA expects to receive a SAML assertion passed through the SSL connection as part of its authentication process. In the ShibGrid Project this required large changes to the Portal and introduced a dependency on the Shibboleth libraries. The Credential Translation Service (CTS see WP3) possess the necessary Shibboleth libraries to allow the modifications to be completed on the CTS rather than on the Portal with much less impact on the Portal/user interface developer. We therefore propose to provide all the Shibboleth mechanisms through the CTS, freeing up the portal/user interface tools to function without requiring the relatively heavyweight Shibboleth Apache Service Provider Infrastructure.

Deliverables:

- Production MyProxy CA service
- CTS MyProxy Interface
- MyProxy policy document

Work-Package 3: Shibboleth based VOMS Front-end

Description: The ability to obtain an X.509 credential from a MyProxy CA does not in itself enable an individual to make use of grid resources instead it provides these resources with the ability to identify the individual. This work package will take the Credential Translation Service (CTS) from the SHEBANGS project and extend it to talk to existing VOMS servers using the identity credentials obtained by the CTS on behalf of individual.

The Credential Translation Service (CTS) developed by the SHEBANGS project, provides a service for translating an Identity Provider's SAML assertions, obtained through browser based Shibboleth methods, into Globus Security Infrastructure (GSI) credentials for use within existing grids, primarily through existing grid portals.

During the authentication process of an individual, the CTS obtains a short term X.509 credential from the MyProxy CA (WP 2). Using this credential it obtains a VOMS Attribute Certificate from the VOMS server specified by the individual. A GSI credential incorporating the VOMS Attribute Certificate is then manufactured and this is delegated to the UK NGS MyProxy server where it is accessible to the

Individual directly or via a Portal. A portal able to obtain this credential is then able to access grid resources on behalf of an individual, enabling existing VOMS-aware grid middleware to make authorisation decisions. Middleware that is not yet VOMS-aware treats the VOMS GSI credential as if it were a vanilla GSI credential by ignoring the VOMS attributes.

It is proposed to develop the CTS to provide a production level service. Figure 1 shows the basic architecture that will be deployed: Step 1 provides the Portal-user the ability to use the SARoNGS mechanism to login. Steps 2, 3 and 4a are the familiar Shibboleth authentication and attribute passing mechanisms. Step 4b shows the ShibGrid style certificate issuing process. Step 4c shows the gathering of VO credentials (VOMS Attribute Certificates). Step 4d shows the SHEBANGS style movement of the credentials into a controlled public credential store (MyProxy). Steps 5, 6 and 7 show the familiar grid Portal access mechanisms.

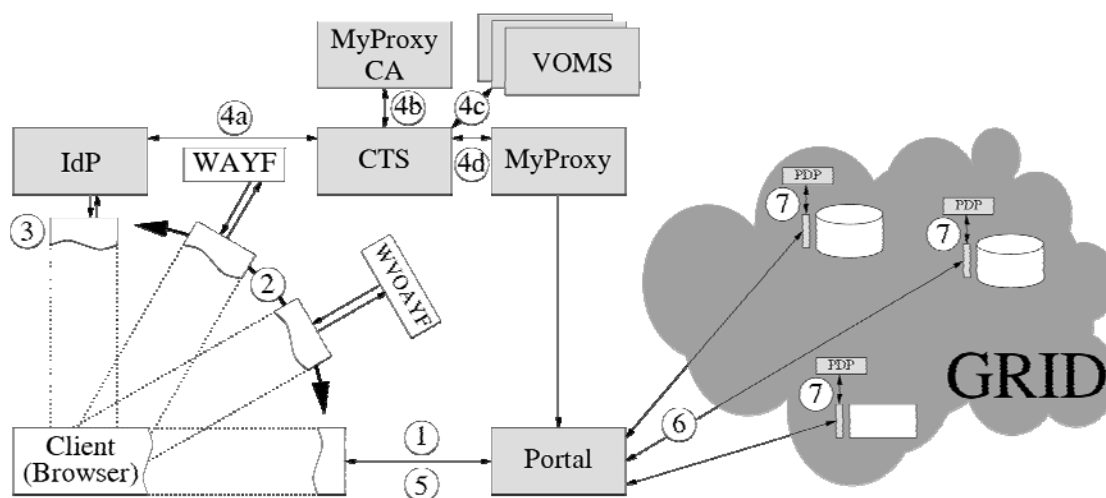


Figure 1 Basic SARoNGS architecture.

The CTS will be further extended to provide a Web Service API (figure 2) that will enable existing portals or other user-facing tools, to be enhanced to support authentication to the grid using Shibboleth derived identity credentials.

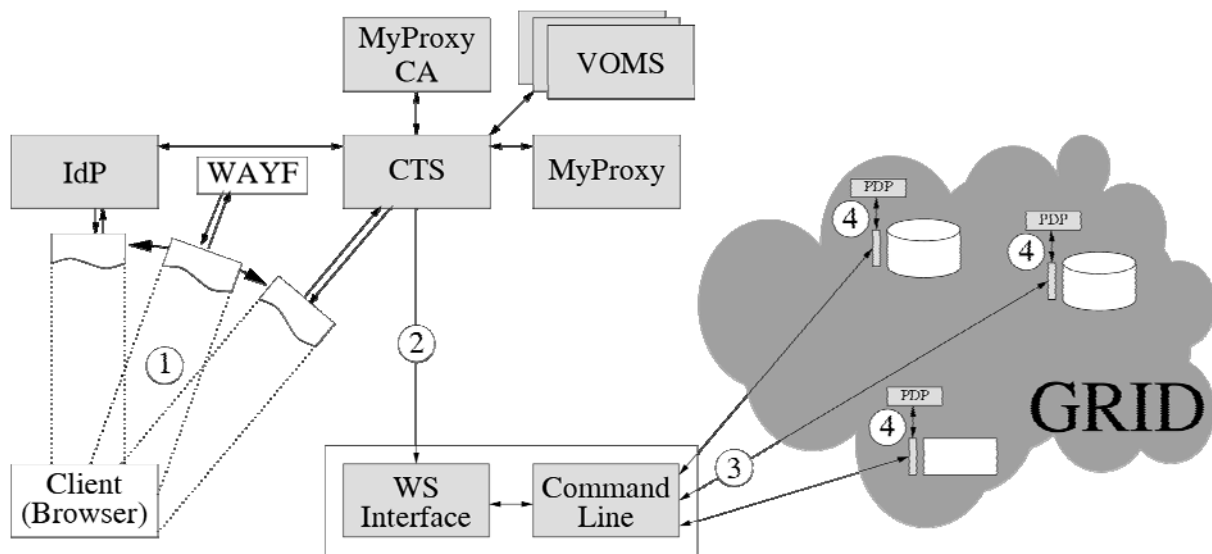


Figure 2 Command line access to the CTS.

Deliverables:

- Internal library to obtain VOMS Attribute Certificates from a VOMS server
- Deployed basic production CTS
- Documentation for portal developers.

Work-Package 4: VO Registration Interface

Description: VOMS authorisation is based on Attribute Certificates generated and issued by the VOMS server to a particular individual identified by their X.509 credential. This project intends to issue certificates without, a priori,, a priori, prior knowledge of an individual and so without having seen their credentials before; in fact it aims to create credentials on the fly. To satisfy the requirement that no private keys need be maintained by the individual this project needs to produce an interface that is able to handle VO registration on behalf of the individual. Figure 3 illustrates how the SARoNGS CTS is able to handle new user registrations. Step 1 shows a user attempting to use a Portal. Steps 2 and 3 are the familiar Shibboleth authentication steps. Step 4 shows the user accessing the Registration Interface (part of the enhanced CTS). The Registration Interface has access to the user's temporary identity credential and with its VOMS libraries is thus able to register the user with the VO of the user's choice.

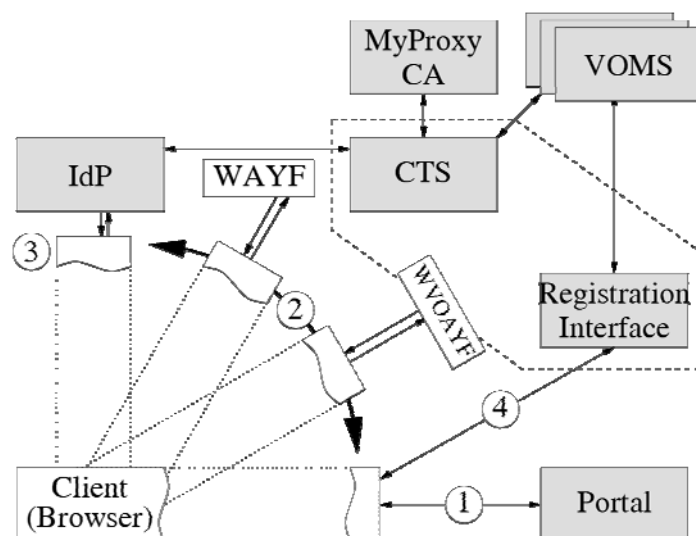


Figure 3 VO Registration via the CTS

Deliverables:

- CTS front-end which allows users to register for VO membership to external VOs
- VO managed CTS front end registration (see WP5)

Work-Package 5: CTS based Virtual Organisations

Description: The maintenance of a VOMS server to host VOs is a heavy-weight task. It is only able to provide attributes to individuals based upon their grid identities. The CTS, on the other hand, is able to provide a more direct route between the Shibboleth based federations and grids. It is a lightweight PERL based CGI program and is therefore easily deployed. A Virtual Organisation may prefer to host a CTS rather than a VOMS service so as to achieve authorisation based on individuals' roles, it may wish to retain anonymous access, it may even wish to use more complex policies based on attributes such as institution, authentication Level of Assurance, or any number of attributes that may be supplied by an Identity Provider.

This package will further develop the CTS to call out to PERMIS for a policy based decision. It will provide a database of users (for data to be held at each user's request) to aid the experience during multiple sessions.

Deliverables:

- PERMIS call-out from CTS
- Membership database extension

Work-Package 6: Developing VOMS-aware services

Description: SARoNGS enables a user to access resources where there is no prior direct relationship between the user and the grid resource provider. The entity, or Virtual Organisation, that hosts the Credential Translation Service or VOMS has prior relationships with the user (perhaps via his IdP or federation) and the resource providers. It is this entity that we rely on to assert the end user's rights to the providers' resources, in the form of a VOMS proxy. We need therefore to consider the readiness of current and future middleware, as run by providers such as the NGS, to make authorisation decisions based on attribute assertions carried by the VOMS proxy. The VPMAN project

has already produced a solution to integrate VOMS and PERMIS such that GT4 based middleware (which is planned for adoption by the NGS) can consume and base authorisation decisions on the proxy provided by an end user. Solutions are also being developed to work with the current NGS job submission mechanism, both using emerging solutions based around LCAS and LCMAPS.

The particular scenario that we address comes from the JISC-funded GEMS project (Grid-Enabling MIMAS Services). Here, the end-user launches a grid job which will in turn read data from a grid-enabled dataset hosted by MIMAS and the NGS. The job authenticates to the service using a proxy credential delegated to it by the user. The data is confidential, and access must be restricted to jobs acting on behalf of users who have registered with, and been approved by, the data owner, a third party. Shibboleth-based mechanisms are already in place to allow a data portal (a Shibboleth SP) to interrogate the data owner to determine whether a Shibboleth-authenticated user has the requisite privilege. Unfortunately, this protocol, designed for use when the user is connected to the portal via a Web browser, is not applicable here, and alternative solutions must be found. We propose to solve the problem by (1) using methods to delegate a VOMS proxy to the job, and arranging that this proxy carries attribute assertions from the data owner concerning the user's rights to access the data, as well as the VO membership assertions that convey the user's rights to execute a job on the grid resources, and (2) using PERMIS to make the authorisation decision within the grid-enabled data services, which will be Web Service based and therefore able to be controlled by outputs from the VPman project.

Deliverable:

- Exemplar service developed initially at MIMAS installed and hosted NGS resources
 - Hosting of geo-spatial satellite data within the NGS data infrastructure
 - A Grid enabled Web Coverage Services (WCS), Web Map Service (WMS), to provide interface to this data.
 - Evaluation and installation of suitable geo-spatial processing tools across the NGS core nodes
 - Grid enabled client tools (e.g. the use of a GridRelay developed by the GEMS-II project)
- A paper describing the approach and implementation experiences in sufficient detail to permit emulation by others facing similar problems.
- Production deployment of PERMIS from VPMan project.

Work-Package 7: Future recommendations: Access Management Federation Scoping

Description: Currently the UK Access Management Federation is drawing up recommendations on which of the standard attributes will be exposed by compliant identity providers. It is currently not clear if these will be sufficient for grids and virtual organisations. Using the existing NGS partner institutions we will capture a full list of the attributes considered as essential for virtual organisation management. We will also document a best practice of this type of ad-hoc matching for future use. The MIMAS partner will develop this as an output from the project, and this will involve ja.net as a stakeholder.

Deliverable: Report on best practise and schema for shib-VO attribute matching submitted as e-Framework GUIDES.