



Project Document Cover Sheet

Before completing this template please note:

- This template is for completion by JISC funded project managers
- Text in italics is explanatory and should be deleted in completed documents.
- Please check with your programme manager before completing this form whether they would like to use a specially adapted template specific to your project.
- Please see Project Management Guidelines for information about assigning version numbers.

Project Information			
Project Acronym	FOAF+SSL+SHIB		
Project Title	Identity & Access Management using Social Networking Technologies		
Start Date	01/01/2010	End Date	30/09/2010
Lead Institution	The University of Manchester		
Project Director			
Project Manager & contact details	Mike Jones Address: Research Computing Services, The University of Manchester, Manchester M13 9PL Email: mike.jones@manchester.ac.uk Tel: +44 161 275 7038 Fax: +44 161 275 6120		
Partner Institutions			
Project Web URL	Web: http://www.rcs.manchester.ac.uk/research/FoafSslShib Wiki: http://wiki.rcs.manchester.ac.uk/community/FoafSslShib		
Programme Name (and number)	<i>Access and Identity Management: Innovation 08/09</i>		
Programme Manager	Chris Brown		

Document Name			
Document Title	<i>Project Plan</i>		
Reporting Period			
Author(s) & project role	Mike Jones, Project Manager		
Date	16/02/2010	Filename	projectplan-FOAF+SSL+SHIB-1.0.odt
URL			
Access	<input checked="" type="checkbox"/> Project and JISC internal		<input type="checkbox"/> General dissemination

Document History		
Version	Date	Comments
1.0	16/02/2010	First draft, to be updated at the end of WP1



JISC Project Plan

Overview of Project

1. Background

Many authentication mechanisms used in eResearch environments introduce a significant barrier to access.

- Traditional PKIs such as that which is used by the NGS provided through the UK e-Science Certificate Authority introduces an independent centralised registration system that many deem overly complex to address the needs of the majority of researchers across the UK.
- Federated Identity Management systems based for example on Shibboleth such as the the UK Access Management Federation devolve registration to a number of member organisations. However, firstly, these organisations are often unable to release enough information about their registrants to provide anything more than direct role based access control; secondly, membership is limited by the normal business restrictions of that organisation and therefore cannot cater for visitors and other ephemeral trust relations.
- Other less complex systems have generally been recognised as inappropriate in large-scale on-line environments due to issues of scale and limits of authority.

This project seeks to apply social networking technologies implemented via the Semantic Web to support identity management.. The proposed system does not prevent the use of a hierarchical trust system such as PKI but its greater potential for devolution offers a more streamlined, and much more usable, alternative. It will demonstrate how current identity and access control systems may benefit from the use of social trust models. The technology will be based on Friend-of-a-Friend (FOAF) – a vocabulary to provide information about people and organisations and describe their relationships.

2. Aims and Objectives

The Project aims to investigate the benefits of using social Networks as a basis for identity management in the eResearch domain. It will merge social networking technologies with current federated identity management systems to demonstrate more flexible, transient, *ad hoc* relationships between people, such as those formed for the purpose of a specific project (i.e. virtual organisations) and can therefore include individuals who would otherwise fit with difficulty in the hierarchy of institutions such as foreign guest researchers or external consultants. The technology will be applied to core middleware utilised by two important JISC initiatives which rely heavily on the Access and Identity Management programme: the UK NGS and the UK Access Management Federation.

3. Overall Approach

The project is divided into three main phases:

1. Requirements gathering phase where the team will research and identify what can be verified and subsequently expressed to a reliant eResearch environments.
2. Implementation Phase: In this phase two development strands will run concurrently
 1. The development of a Shibboleth Identity Provider which uses FOAF+SSL in place of more traditional IdP registration. Attributes released to any Federated Identity Management system will be based upon an individuals Social Network.
 2. The development of a pluggable authorisation module into Globus based grid resources allowing direct access using FOAF+SSL credentials

3. Evaluation and documentation phase where the team will expose the developed access control mechanisms, and work with NGS and Federation.

4. Project Outputs

1. Revised Plan based upon output of requirements gathering exercise.
2. Project Website
3. A Shibboleth IdP suitable for inclusion in the UK Access Management Federation, where assertions will be verified and released as SAML assertions
4. Authorization plug-in module for Globus
5. Installation Documentation
6. Final Report containing the outcomes, evaluation results and lessons learned.

5. Project Outcomes

This project is expected to be of great value to the future Academic user community and therefore JISC through its engagement with the NGS and the UK Access Management Federation its members and users. It focusses on the call's Cross Themes:

Technology & Tools: Where we plan to develop an IdP framework and a Globus toolkit authorisation plug-in both licensed and available under an open source license.

Interoperability: Where we plan to integrate and demonstrate FOAF+SSL mechanisms working in two existing JISC-funded production environments.

Through development of practical demonstrators, the project will explore the space of user controlled attribute assertions and will be able to thus report experiences and lessons learned in the implementation of such a system. By addressing the issues and requirements highlighted in the call as described above, this project will be evaluating possible solutions to address known and perceived inadequacies in current production systems of the UK's two main Academic AIM infrastructures, providing solutions that can be plugged directly into these eResearch Computing infrastructure. It is envisaged that this will not only benefit the infrastructure providers but also the service providers through more tunable security models.

6. Stakeholder Analysis

Stakeholder	Interest / stake	Importance
JISC	Funding Body	High
NGS	Greater Access to resources.	High
	Management of dynamic VOs.	Medium
UK Access Management Federation	Users' Attributes.	High
	Attribute Release Policy.	Medium
	VO/Inter-Organisational Attributes.	High
Resource Owners	Security/Access Management	High
End Users	Reduction of barrier to entry.	High
	Dynamic VO formation.	Medium - High
	Organisational Independence.	Medium

7. Risk Analysis

Risk	Probability (1-5)	Severity (1-5)	(PxS)Score	Action to Prevent/Manage Risk
Staffing	2	4	8	Only limited resources are available from the project; however, existing staff members with relevant skills from Research Computing Services have been coopted on to the project.
External suppliers and colaborators	2	2	4	No external suppliers involved. We intend to fully engage with the developers of FOAF+SSL. We identify that the lead developer is employed by Sun Microsystems and may be required to refocus his efforts elsewhere. However, Reserch Computing Staff at Manchester have been involved in the writing of FOAF+SSL since the early stages of its development and should be able to satisfactoraly complete the tasks described in this project.
Policy	4	2	8	Policy protecting the day-to-day operation of the Access Management Federation and the NGS may conflict with procedures required to operate FOAF+SSL based systems in these environments. However, this project is not aiming to put into production these service but to explore the benefits and impacts and flaws of such systems in these environments. The project will seek feedback from the NGS and to this end has arranged monthly representation at the NGS R&D meeting for the duration of the project.
Sustainability	1	1	1	The project is focussed on the demonstration of a technology as a solution to problems highlighted by JISC. Results and software will continue to be available after the end of the project should JISC, The UK Access Management Federation or the NGS wish to make further use for outputs from this project.

8. Standards

Name of standard or specification	Version	Notes
X.509	3	Simple Self Signed Certificates are used in FOAF+SSL
TLS/SSL	1.0(3.1) / 3.0	We rely upon already existing implementations of the Transport Layer Security
GSI	All	We rely upon already existing implementations of GSI
SAML	1 and 2	SAML will be used for both the IdP and for the Globus Authorisation call-out
XACML	2	Will be used to express access to grid resources.
FOAF / RDF	N/A	RDF will be used to Interpreted to ascertain the structure of the underlying social Network.

Project Acronym: FOAS+SSL+SHIB
Version: 1.0
Contact: Mike Jones mike.jones@manchester.ac.uk
Date: 16/02/2010

9. Technical Development

An iterative, agile software development approach will be undertaken during the development phase. Software will be maintained via GitHub.

10. Intellectual Property Rights

All project outputs will be made available, free at the point of use, to the UK HE and FE community in perpetuity in the knowledge that these may be disseminated widely in partnership with JISC. These outputs will be made available under an attribution only based open source licence allowing JISC or its representatives to utilise, archive and disseminate the work.

Project Resources

11. Project Partners

The team will liaise with Henry Story, a Social Web Architect at Sun Microsystems, who is the leader of the FOAF+SSL project and an expert in Semantic Web technologies, as well as a participant of the W3C Social Web Incubator Group. No formal arrangements are deemed necessary other than to cover travel and expenses.

12. Project Management

The project will be managed and administered by the Project Manager, Mike Jones, whose role it is to maintain strategic direction for the project; to monitor progress of project activities; to initiate remedial action because of slippage or in the event of risks occurring; to provide a single point of contact for the project; to ensure the full engagement of all stakeholders through effective implementation of the dissemination work package; and to lead the production of JISC progress and final reports. The Project Manager is assigned to the project at 10% FTE.

The technical direction of the project is the responsibility of the Lead Developer, Bruno Harbulot, whose role it is to track the developments in the FOAF+SSL project, to advise the project manager on all matters relating to the technical strategy of the project, provide guidance for other members of the project team as well as to develop and evaluate the shibboleth deliverables.

Robert Frank, grid security officer working on the NGS project will be co-opted onto this project after the initial requirements gathering phase. His role (Developer) will be to develop and evaluate the authorisation plug-in to the NGS grid middleware.

13. Programme Support

For the outputs of this project it is important to maintain connection with the primary stakeholders. NGS and UK Access Management federation. We therefore request that these stakeholders are invited to any JISC AIM meetings during the running of this project.

14. Budget

See Appendix A.

There has been no change to the overall budget as submitted as part of the proposal. The omission of Indirect Costs line as advised to JISC 15/12/2009 has been introduced back into the document.

Detailed Project Planning

15. Workpackages

The Planned Workpackages can be found in Appendix B.

Page 5 of 11

Document title: JISC Project Plan

Last updated: April 2007

16. Evaluation Plan

Timing Month	Factor to Evaluate	Questions to Address	Method(s)	Measure of Success
9	Integration into shibboleth protected Authorisation system	Is it possible to obtain a Shibboleth Assertion based upon FOAF+SSL which can be used for authorisation to a web based services.	Set-up a number of services with access policies based upon differing asserted attributes and relationships	Ability to demonstrate access granted and denied.
9	Integration into grid based authorisation decision	Is it possible to gain access to grid enabled resource using FOAF+SSL authentication.	Configure a GRAM and GSIFTP service to use Plugin.	Ability to demonstrate access granted and denied.

17. Quality Plan

Output	Shibboleth IdP				
Timing Month	Quality criteria	QA method(s)	Evidence of compliance	Quality responsibilities	Quality tools (if applicable)
8	Robustness	jUnit testing	Passes all tests	Lead Developer	
8	Adherence to standards	Interoperation	Working demonstration	Lead Developer	
3-9	Fit for purpose	Review of Federation documentation	Ability to express Social Network through Shibboleth	Lead Developer	

Output	Globus Authorisation Plugin				
Timing	Quality criteria	QA method(s)	Evidence of compliance	Quality responsibilities	Quality tools (if applicable)
8	Robustness	jUnit tests, Demonstrator		Developer	
8	Adherence to standards	Interoperation	Ability to use standard grid tools	Developer	
3-9	Fit for purpose	Steering by NGS	Consensus	Developer	

18. Dissemination Plan

Timing	Dissemination Activity	Audience	Purpose	Key Message
End of Project	Presentation/Demos at All Hands Meeting	eResearchers and technologists	Demonstrate value of Social Networks as a means of Identity Management	Ease of access, Dynamic VO formation, Identity Management without barriers
Ongoing	Continued meeting at NGS R&D meetings	NGS technologists	Steering and information exchange	Technical details
As arranged by JISC	Presentations at JISC AIM Meetings	AIM sibling project members, UK AMF	Present both Shibboleth and Grid sides of the project	Ease of access, Dynamic VO formation, Identity Management without barriers

19. Exit and Sustainability Plans

The project aims to produce two demonstrator applications in order to explore the suitability of FOAF+SSL as a form of user centric authentication and community authorisation. A further deliverable of the project will be an evaluation report. The project will place copies of the code in a publicly available code repository for no less than three years beyond the end of the project. Engagement with the open-source software communities will be made from the start, provided that a suitable licensing agreement is chosen. In fact, proposed members of the team have been involved in the development of FOAF+SSL implementations from its inception, all of which have been published and/or contributed to the appropriate open-source project. Early involvement with existing well-established open-source projects will strengthen the sustainability of the output of this project.

Project Outputs	Action for Take-up & Embedding	Action for Exit
IdP Demonstrator	This is an independent IdP and will be available for subsequent uptake either by institutes and/or open source communities.	Make available software and documentation.
Globus Plugin Demonstrator	Installer for demonstrator to be made available as a pluggable authentication module compatible with the NGS software stack.	Make available software and documentation.

Project Outputs	Why Sustainable	Scenarios for Taking Forward	Issues to Address
IdP Demonstrator	Discrete item of software	Software maintenance potentially via open source community	
Globus Plugin Demonstrator	Discrete item of software	Software maintenance potentially via NGS	

Appendixes

Appendix A. Project Budget

Directly Incurred Staff	January 10 – March 10	April 10 – March 11	TOTAL £
Post, Grade, No. Hours & % FTE			
Mike Jones, gd 6, 10%			
Robert Frank, gd 5, 50%			
Bruno Harbulot, gd 6, 50%			
Total Directly Incurred Staff (A)			
Non-Staff	January 10 – March 10	April 10 – March 11	TOTAL £
Travel and expenses	£833.00	£1,667.00	£2,500.00
Hardware/software	£500.00	£	£500.00
Dissemination	£	£	£
Evaluation	£	£	£
Other Consultancy	£4,500.00	£	£4,500.00
Total Directly Incurred Non-Staff (B)	£5,833.00	£1,667.00	£7500
Directly Incurred Total (C) (A+B=C)			
Directly Allocated	January 10 – March 10	April 10 – March 11	TOTAL £
Staff	£	£	£
Estates	£3,644.00	£7,289.00	£10,933.00
Other	£	£	£
Directly Allocated Total (D)	£3,644.00	£7,289.00	£10,933.00
Indirect Costs (E)	£9,211	£18,421	£27,632
Total Project Cost (C+D+E)	£28,889.00	£47,779.00	£76,668.00
Amount Requested from JISC	£23,111.00	£38,223.00	£61,334.00
Institutional Contributions	£5,778.00	£9,556.00	£15,334.00
Percentage Contributions over the life of the project	JISC X 80%	Partners X 20%	Total 100%
No. FTEs used to calculate indirect and estates charges, and staff included	No FTEs 1.1 FTE	Which Staff: All Named above	



Appendix B. JISC WORK PACKAGE

WORKPACKAGES	Mont	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0:	1-9	X	X	X	X	X	X	X	X	X															
1:	1-2	X	X																						
2:	3-8			X	X	X	X	X	X																
3:	3-8			X	X	X	X	X	X																
4:	8-9									X															

Project start date: 1 January 2010

Project completion date: 31 September 2010

Duration: 9 months

Workpackage and activity	Earliest Start Date	Latest completion date	Outputs (clearly indicate deliverables and reports in bold)	Milestone	Responsibility
YEAR 1					
WORKPACKAGE 0: Project Management					
Objective: To over see the smooth running of the project					
1. Project Management	01/01/10	30/09/10	JISC Required Documents		MJ
			Project Website and Wiki		BH

<p>WORKPACKAGE 1: Requirements Gathering</p> <p>Objective: to analyse the FOAF semantics and derive a formulation to express common authorisation assertions acceptable to on-line service within the UK Access Management Federation, NGS and wider research computing infrastructures. Meetings will be held initially face to face and continually throughout the project between the active FOAF+SSL members and consultants.</p>					
2. Analysis of FOAF Semantics	01/01/10	28/02/10	List of Attributes, Revised Workplan		BH
<p>WORKPACKAGE 2: FOAF Hosting Site and FOAF+SSL IdP</p> <p>Objective: Develop a Shibboleth IdP based upon validated assertions made by the user via their FOAF file.</p>					
3. FOAF+SSL URI Environment	01/03/10	15/03/10	FOAF+SSL web site (for authentication)		BH
4. FOAF+SSL IdP	15/03/10	31/08/10	FOAF+SSL Identity Provider		BH
<p>WORKPACKAGE 3: FOAF+SSL Globus Integration</p> <p>Objective: Since Globus relies on certificate-based SSL connections, this package aims to explore the process of delegation via the Globus Authorisation call-out mechanism. An authorisation library will be created to process FOAF+SSL connections and provide authorisation based initially on VO assertions for the Globus preWebService GRAM Job submission service.</p>					
5. FOAF+SSL Authorisation Plugin	01/03/10	31/08/10	Globus Authorisation plugin		RF

WORKPACKAGE 4: Evaluation and Documentation				
Objective: Installation Review, Performance Evaluation and Documentation				
6. Software Performance review	01/09/10	31/09/10	Report to be included in the final report	BH/RF
7. Installation documentation	01/09/10	31/09/10	Two Documents	BH/RF
8. Installation evaluation and suitability	01/09/10	31/09/10	Report to be included in the final report	BH/RF

Members of Project Team:

MJ = Mike Jones

BH = Bruno Harbulot

RF = Robert Frank