



Joining the UK Access Management Federation

Version 1.3

Prepared by:

Simon Bilton
Simon.Bilton@salfordsoftware.co.uk
0161 906 1002

Additional Contributions by:
James Blake
James.Blake@salfordsoftware.co.uk

18th June 2007

Salford Software
Lancastrian Office Centre
Talbot Road
Old Trafford
Manchester
M32 0FP

Contents

Contents.....	2
1 Background	3
2 Project Plan	4
3 Benefits of packaged Solution	11
4 Packaged Solution Options	12
Basic Option*	12
Advanced Option	12
Institutional Audit	13
Custom Option.....	13
5 Contracting out Joining The UK Access Management Federation	14
7 Deliverables	15
8 Benefits of Solution	18

1 Background

JISC have produced a “road-map” for joining the UK Access Management Federation, this consists of six steps. Salford Software has produced a corresponding service to assist institutions deliver each of the six steps in this road map, these are detailed on the following pages.

Salford Software specialises in the provision of Identity solutions for the academic community in the UK. In particular, Salford Software has vast experience of directory systems and associated security services.

Using this knowledge, Salford Software is able to work with institutions to help them with the development of the various services required to participate in the UK Access Management Federation.

Furthermore, Salford Software work very closely with the various organisations involved with the instigation and control of the new services, notably JISC, BECTA and JANET(UK), formerly UKERNA.

Salford Software is among the early adopters of UK Access Management Federation services.

Salford Software also engages with key vendors such as Microsoft, Novell and SUN to develop services that can be used to deliver suitable solutions to enable institutions to join and utilise the resources provided through the UK Access Management Federation.

With the necessary technical skills and strategic partnerships with these key organisations and the experience of having already delivered Identity and Secure Access systems to many institutions, Salford Software is ideally suited to deliver the best solution for accessing the UK Access Management Federation.

This document outlines the steps of joining the UK Access Management Federation and how Salford Software can assist.

2 Project Plan

Step 1 - Institutional Audit

Review: "Institutions should carry out an audit to review readiness to adopt federated access management. This would include making a choice between the three strategic JISC options* and alignment with institutional information strategy."

Salford Deliverables

This exercise involves an experienced consultant investigating any existing directory services or other user data that could be utilised as the source for the identity-based attributes required to access federated resources via the Shibboleth protocol.

Activities will include:

- Meeting with key stakeholders to establish short and long term business requirements (including Athens Administrator)
- Review of skills sets and preferred platforms and technologies
- Review of Directory Services
- Review of present Authentication mechanisms
- Identify preparatory tasks that must be completed
- Review of current Athens access
- Indicative budget to deliver Institutions preferred approach

The overall deliverable will be a report describing the existing services, their suitability for use as the source for providing the Shibboleth attributes, identification of any preparatory tasks and finally a recommendation of which of the JISC options* to implement to provide access to the Federated services.

Pre-Requisites

The on-site element will require access to appropriate resources at the institution such as the current Athens administrator, directory services administrator, and potentially the Student Record System administrator.

*JISC Options

BECOME A FULL MEMBER OF THE FEDERATION USING COMMUNITY SUPPORTED TOOLS

- COSTS: Institutional effort to implement software, join federation and enhance institutional directories
- BENEFITS: Full institutional control, skilled staff and access management solution for internal, external and collaborative resources

BECOME A FULL MEMBER OF THE FEDERATION USING TOOLS WITH PAID-FOR SUPPORT

- COSTS: Cost of support from supplier and institutional effort in liaison with supplier and federation
- BENEFITS: Full support in implementation and access management solution for internal, external and collaborative resources

SUBSCRIBE TO AN 'OUTSOURCED IDENTITY PROVIDER' TO WORK THROUGH THE FEDERATION ON YOUR BEHALF (SUCH AS USE OF CLASSIC ATHENS WITH THE GATEWAYS)

- COSTS: Subscription costs to external supplier (from July 2008) and internal administration role
- BENEFITS: Minimum institutional effort to achieve access to external resources only

Step 2 - Directory Development

Develop: “Directories need to be correctly populated with attributes about students and staff that meet the federation standard known as the EduPerson.”

Once the Institutional Audit has been carried out and the strategy for connecting to the federation has been determined, it will be necessary to carry out some work on the selected directory system to enable support for the EduPerson attributes.

This work will vary enormously between institutions, dependant on the current status of the identity platform. Some institutions will be in a position to simply add the attributes into their current directory service, whereas others may need to implement a full Identity Management (IDM) solution, which is a major piece of work in its own right.

It should be pointed out that a full IDM solution is not a pre-requisite for joining the UK Access Management Federation, although those early adopters that already had a sound Identity platform found the implementation much easier.

Salford Deliverables

This process will vary between institutions, but the deliverable will be an identity source that will meet the requirements to provide the required data via the EduPerson attributes necessary for using the UK Access Management Federation services. This source is likely to be a directory service (e.g. eDirectory, Active Directory, OpenLDAP etc) but could be a database. The Identity source must also be developed to ensure that the contents are accurate and regularly maintained in order to meet the UK Access Management Federation policy.

Pre-Requisites

Salford will require access to appropriate resources at the institution such as the current Athens administrator, directory services administrator, and potentially the Student Record System administrator. An institutional strategy for Athens usage should be in place (i.e. does every user have access to all services, or is there more granular access based on staff/student status, course membership etc.)

Duration

Variable, dependant on solution

Step 3 - Authentication Development

Choose and Implement: “An institutional authentication, or single sign-on, system should be selected. Institutions can choose from commercial or open source products.”

In order to utilise Shibboleth, an institution must deploy a suitable web-based authentication service. There are many solutions available to meet this requirement, the choice should be made in accordance with the directory service selected in step 2. Solutions can be implemented to service only the Shibboleth requirements, or could be extended to deliver Single Sign-On to additional resources, be they internal or external.

Solutions could be Open Source or commercial products

Salford Deliverables

Salford will work with the institution to assess, recommend and deliver an appropriate authentication service. If an existing service is in place, Salford will assess the suitability of that service to deliver the requirements for UK Access Management Federation.

If additional resources are to be serviced, they will be considered additional tasks.

Pre-Requisites

The institution should make their stance on the use of Open Source software known to Salford. Also, if commercial products are to be considered, an indication should be given of available budget.

Any security policies should be presented, and any requirement for more additional security (e.g. multi-factor authentication) should also be made known at this time.

Step 4 - Implement IdP

Choose and Implement: “The fourth stage is to implement Identity Provider software. Institutions can currently choose between the Shibboleth, AthensIM and Guanxi implementations.”

The choice of the IdP software solution will be determined based on the directory and authentication services delivered in steps 2 and 3.

At this time there are no commercial products which meet entirely the requirements for the IdP, and therefore one of the Open Source solutions is likely to be required.

Salford Deliverables

Salford will work with the institution to select the most appropriate software. Salford will then install and configure the chosen application to integrate into the authentication and directory solutions from steps 2 and 3.

Pre-Requisites

Completion of steps 2 and 3. In order to finalise the service, step 5 (Join the federation) must also be completed.

Step 5 - Join the Federation

Action: "All institutions who wish to participate will need to join the UK federation by registering and agreeing to observe federation policy."

The institution needs to join the federation in accordance with the documentation available at the following locations:

- www.ukfederation.org.uk/content/Documents/JoinFederation
- www.ukfederation.org.uk/content/Documents/ApplyforMembership
- www.ukfederation.org.uk/content/Documents/RegisterIdP

Salford Deliverables

It is normally the institution's responsibility to complete these tasks in a timely manner.

However, as part of the packaged solution described here, Salford can act as an "agent" for the institution and liaise with the appropriate authorities on behalf of the institution - the exception to this being the initial letter of application, which must be signed by a senior representative of the institution.

Pre-Requisites

The IdP installation can only be completed once the institution has fully registered with the UK Access Management Federation.

Step 6 - Institutional Rollout

Action: "On becoming a member of the federation, an institution will need to roll out the new system. This may include staff training and development of new user guides and support mechanisms."

The roll out of the new system will vary from institution to institution. Some key points to note include:

- Alteration of hard-coded URLs on static web pages
- Changes to user documentation (user guides etc)
- Training and Support

Salford Deliverables

Salford will provide training to the institution's technical staff to ensure they understand the technologies behind any new products involved in the final solution. Salford will also offer support services for the deployed system.

Pre-Requisites

Successful testing, development, deployment and documentation of the new services

3 Benefits of packaged Solution

Salford Software will guide the institution through the UK Access Management Federation.

Institutions do not have to spend valuable time learning about the intricacies of the IdP Shibboleth software.

Technical staff will be trained to support the key components of the solution.

The solution is fully supported by Salford Software.

The fixed price compares favourably with other offerings and the solution allows the institution to retain management and ownership of the environment.

4 Packaged Solution Options

All solutions are provided with 12 months telephone for the solution, including remote access where required. Escalation to on site and non essential updates are not covered.

Basic Option*

Assistance with joining UK Access Management Federation (acting as an agent for the institution)

Installation and configuration of Linux-based Shibboleth IdP software

Integration of Directory services (or alternative database) with IdP

Configuration of basic web authentication service using IdP

Registration of IdP entities

Testing against Shibboleth-protected resources

Technical handover to institution

Advice on Institutional roll-out

*Requires suitable Directory Service

Total Cost	£4995
Annual Support	£695 pa

Advanced Option

As above but includes Institutional Audit and report

Total Cost	£8495
Annual Support	£695 pa

Institutional Audit

The Institutional Audit has two options - single and complex, depending on the number of directory services. The deliverable is a comprehensive report identifying the suitability of the existing services for use Shibboleth, covering topics such as security, richness and accuracy of data, management of account provisioning and de-provisioning, and a recommendation of the most appropriate IdP solution.

Multiple Directories

£2795

Custom Option

If work is required on either Directory services or the Web Single Sign-On components, additional costs will be incurred.

Total Cost

£POA

All prices quoted exclude VAT.

5 Contracting out Joining The UK Access Management Federation

Based on feedback from the community, it has been recognised that some institutions would prefer to outsource the entire registration process and deployment of the IdP solution. Reasons for this include:-

- Internal Resource Limitations
- Skill Set
- Support
- Administrative Overheads
- Simplified Sign On

Consequently, Salford Software have entered into an agreement with the UK federation which allows Salford Software to be delegated the authority to carry out the various registration and installation tasks on behalf of an institution.

7 Deliverables

This solution will only deliver steps 3, 4 and 5 of the JISC roadmap. In order to maximise the efficiency of the delivery, the following tasks are carried out.

Task 1a

Assist the institution with identification of the Executive and Management Liaison contacts.

Assist the Executive Liaison with the production of the letter of application to join the UK federation, including explanation of the rules of the federation where necessary.

Provide a customer pack containing the UK federation rules and policies along with the sample letter

Task 1b

Establish the institution's position regarding X.509 certificates. If necessary, assist the institution through the application process for a suitable certificate from a supported Certificate Authority (see <http://www.ukfederation.org.uk/content/Documents/GetCertificate> for list of currently supported CAs).

Task 1c

Confirm that the pre-requisites have been met.

Pre-requisites

In order for Salford Software to deliver this fixed price solution, the institution must meet a certain number of pre-requisites. These are listed below.

Pre-requisite	Description	Guidelines	Responsibility
Attribute Store	A suitable Attribute Store must be available in the form of a directory service or database and it must meet any criteria stipulated by the UK federation or Service Providers therein	The institution must be able to demonstrate that an Institutional Audit has been carried out (either by the institution themselves or another agent). The audit should cover matters such as:- <ul style="list-style-type: none"> • Security • "Richness" of data • Accuracy • Management 	IT

Pre-requisite	Description	Guidelines	Responsibility
		of change	
Federation Rules	The institution must understand and agree to the rules of UK federation, in particular the area of logging, re-use of credentials and accountability	The Executive Liaison enters into a legal agreement with the UK federation and must be aware of the rules	Executive Liaison
Server Platform	The institution must provide a suitable hardware platform (along with any software and license keys) to host the chosen IdP solution. Further consideration should be given to any High Availability or Disaster Recovery requirements	As part of task 1c, the choice of host platform for the IdP will be a logical outcome of the checking process The institution should also check availability of:- <ul style="list-style-type: none"> • Rack Space and Power • Network ports 	IT
X.509 certificate	The institution must be prepared to accept any and all costs associated with acquiring a commercial certificate if required	Most institutions are likely to choose a "free" certificate from one of the Certificate Authorities	IT/Library
Access to Attribute Store	Full administrative access must be provided to the attribute store		IT
Firewall Configuration	Depending on the existing infrastructure, it may be necessary to open certain ports on the firewall	This must be done in advance of the deployment of the software	IT

Task 2

Build the server platform (Linux or Windows) to host the Shibboleth IdP software. Install and configure the Shibboleth IdP software, including Apache and Tomcat, and appropriate connection to attribute store identified as part of task 1c.

The server should be delivered to Salford Software's premises for configuration, and in the case of Windows the appropriate licensing details provided.

Task 3

Register the specific entities, scopes, IP addresses etc with the UK federation, along with remaining named contacts (e.g. support contact).

Task 4

Install the X.509 certificate on the IdP and perform the necessary certificate exchanges with the UK federation.

This will have to take place on customer site to comply with DNS requirements.

Task 5

Test and sign off deployment in accordance with the sign-off sheet in the customer pack.

Task 6

Undertake basic administration training and hand over documentation.

8 Benefits of Solution

The list below shows some of the benefits of the Salford Software solution.

- Salford will guide the institution through the UK federation registration process.
- Institutions do not have to spend valuable time learning about the intricacies of the IdP Shibboleth software.
- Technical staff will be trained to support the key components of the solution.
- The solution is fully supported by Salford Software.
- The fixed price compares favourably with other offerings.
- The institution retains management and ownership of the environment.
- Full documentation set
- Ongoing Research and Development Program
- Proven Track Record

For more information on the UK Access Management Federation, visit:-

<http://www.ukfederation.org.uk>