JISC

JISC Final Report

Project Information			
Project Identifier	*UKDA IdM Toolkit Pilot*		
Project Title	UK Data Archive: Identity Management in a Service Provision Environment		
Project Hashtag			
Start Date	01 February 2011	**End Date**	31 July 2011
Lead Institution	UK Data Archive, University of Essex		
Project Director	John Shepherdson, UK Data Archive, University of Essex, Colchester, CO4 3SQ		
Project Manager	David Hall, UK Data Archive, University of Essex, Colchester, CO4 3SQ,		
Contact email	djhall@data-archive.ac.uk		
Partner Institutions	University of Essex		
Project Web URL	http://www.data-archive.ac.uk/about/projects?id=2892		
Programme Name	Access and Identity Management Programme		
Programme Manager	Christopher Brown		

Document Information			
Author(s)	David Hall		
Project Role(s)	Project Manager		
Date	14 September 2011	**Filename**	UKDAIM-JISC_FinalReport_01-01
URL	http://www.data-archive.ac.uk/about/projects/identity-management		
Access	This report is for general dissemination		

Document History		
Version	**Date**	**Comments**
00.01	07 July 2011	Draft for JISC
00.02	12 July 2011	Updated to incorporate items following JISC feedback
00.03	28 July 2011	Incorporating gap analysis information.
01.00	5 August 2011	Issued version for online publication
01.01	14 September 2011	Final version with urls

Table of Contents

1 Acknowledgements

This project was funded as part of the JISC Access and Identity Management Programme, with valuable support from the University of Essex. It was conducted within the University of Essex by the UK Data Archive in partnership with the Information Services Section.

The success of the project was reliant upon the strong support of the Archive's management and the contribution of all Archive and ISS staff who were interviewed or provided background information for identity management.

Guidance in preparation of case studies and reporting was provided by Chris Brown, AIM Programme Manager, and John Paschoud, Identity Management Toolkit Project Manager.

2 Project Summary

This project tested the audit and gap analysis approaches and methodologies set out in the JISC Identity Management Toolkit in the mixed and complex Identity Management (IdM) environment of the UK Data Archive as a major service provider (SP). The work informed improvements to IdM at the Archive, thereby also delivering benefits for the Archive's main user communities - data creators/owners, data users and the wider academic community. The project was of significance because of the Archive's role working with identity providers (IdP) and acting as a 'virtual orphanage' IdP for users outside the standard higher and further education identity management structure.

The Identity Management Toolkit provides a structure for the assessment and development of identity management in a further and higher education institutional context. Whilst the Toolkit was created and tested within organisations which in essence act as IdPs this project focused on applying the Toolkit approach to review identity management within the UK Data Archive as a SP.

It is clear that a SP faces different identity management challenges because it is be heavily reliant upon information provided by a wide range of IdPs and individual users. The effectiveness of the IdM at IdPs is critical to the level of trust extended by the SP. The Toolkit can be applied in this situation to ensure the SP has robust internal policies and procedures to assure the adequate protection of the resources to which it provides access. It also highlights the risks inherent in accepting IdP and user supplied identity information, allowing the SP to make a proper assessment of the acceptability of those risks.

As a result of applying the Toolkit to audit and gap analysis at a SP it has also been possible to suggest some minor adjustments to the Toolkit so that it can be used more easily. In general what this means is use of the Toolkit should be tailored to the organisation's size and complexity, recognising the environment within which it operates.

3 Project Description

3.1 Project Outputs and Outcomes

Output / Outcome Type (e.g. report, publication, software, knowledge built)	Brief Description and URLs (where applicable)
UKDAIM Identity Management Audit Report	The audit report for the IdM policy and procedures of the UK Data Archive – *http://www.data-archive.ac.uk/about/projects/identity-management*
UKDAIM Identity Management Gap Analysis	A gap analysis report based on the findings of the audit and further investigation of user feedback on services – *http://www.data-archive.ac.uk/about/projects/identity-management*

UKDAIM Identity Management Case Study	A case study covering the use of the IdM Toolkit at the UK Data Archive and referencing the audit and gap analysis reports – *http://www.data-archive.ac.uk/about/projects/identity-management*

3.2   *Project process and methodology*

The project aimed to test application of the Toolkit's approach to IdM review whilst also delivering the benefits of such a review to the Archive. As such it was important to balance following the Toolkit and ensuring any audit and gap analysis delivered value. The project covered -

- The IdM role of the Archive as a SP;
- The IdM role of the Archive in providing Shibboleth credentials for users outside UK F&HE (virtual orphanage)

This meant that, for example, the contact with IdM subjects - users - was adjusted to see if remote users could be effectively canvassed for their views. It also meant that the audit report did not follow the template in the Toolkit, but was set out in a form that took account of both the audience and the corporate style of the Archive. The report did, however, take account of all issues described in the template.

The audit involved the steps laid out in the Toolkit:

- General email contact within the organisation to elicit contributions to the audit (Feb-Mar 2011);
- Targeted email and face to face contact with individuals specifically identified as relevant to IdM (Feb-Mar 2011);
- Targeted email to users (Mar-Apr 2011);
- Interviews (Mar-May 2011);
- Document review (Mar-June 2011).

In addition there was some technical review of the Shibboleth authentication process because of the Archive's unique Virtual Organisation Service Provider. This was to provide a better understanding of the way in which user attributes derived from IdPs were being used to control resource access.

The detailed results of the project are to be found in the three key document outputs from the project - audit and gap analysis reports, and the case study.

3.3   *Project findings*

Reference can be made to the three key document outputs for the findings and recommendations for change which arose from the audit and gap analysis. Of particular note is the importance of clear, comprehensive, but simply structured documentation, in making IdM work effectively in any service provision environment.

It should be clear that SPs must be aware of the reliance and trust they place on the IdM work of those institutions providing IdP services for individuals. It is clear that poor implementation, including technical implementation, of IdM by an IdP can compromise the whole trust process. The Archive has experience of two significant instances (see section 8) of inadequate IdM implementation at UK F&HE institutions, over a three year period, which affected the unique and persistent nature of the identity credentials being presented for individuals. These incidents meant that access to resources could potentially be made by unauthorised or ineligible users. Where a SP delivers resources supplied to it by others the agreements, licences and contracts under which this happens can be adversely affected by such incidents.

The relationship between SP and IdP is complex and it is not clear whether, when assessing their own IdM processes, IdPs consider the impact of their decisions on various external SPs to which their users may want access. For example, there are now many UK F&HE institutions which are, or will be, providing credentials for users at associated institutions overseas. A decision on how to provide those

credentials - through an existing IdP registered with the UKAMF for the UK institution or through a separate IdP registered with the UKAMF for the non-UK users - can be of primary importance to some SPs where their resources may be restricted to access within the UK. It might be useful for IdPs to prepare a matrix of known restrictions and access conditions for SPs with whom their users have any relationship when addressing this issue.

This may not be an issue to be addressed within the Toolkit, but it is an issue for the operation of the UKAMF. This IdP and SP relationship, and the impact on service access, should be a strategic priority for JISC to take forward when licensing content, with an emphasis on the easy reusability of model licences.

As well as being a SP the Archive provides Shibboleth credentials to users outside UK F&HE (acts as a virtual orphanage for these users) to allow them to authenticate via the UK Access Management Federation. The level of checking of the identity of these users is minimal, but the risk to the Archive of allowing unauthorised access to any resources is minimal as these credentials do not allow a user access beyond the generally available resources managed by the Archive. The Archive issued credentials cannot be used to access the resources of other SPs. It is clear that any organisation running a virtual orphanage should have IdM processes appropriate to the number and nature of the services for which it intends to vouch for the user's identity. Similarly, any SP dealing with a virtual orphanage IdP should have particular regard to the trust that can be placed in its IdM policies and processes.

The Toolkit provides a sound basis for review of IdM in a service provision environment, though it might be useful for it to take into account the following issues:

- **The SP and its user community.** For a SP there is a greater degree of remoteness from the consumers of IdM and IdP processes. Obtaining the views of these consumers - users - is problematic. The approach to these users - the mode of contact and the nature of the questions - will be different to that set out in the Toolkit. Obtaining responses from remote users is difficult and it may be that their views might be elicited via social networking and/or short online surveys. It is unlikely that the SP will be able to go beyond an IdP to address the IdP's own consumers.

- **The audit report template.** This is comprehensive, but may not necessarily be the appropriate format for the intended audience. During this project it was felt the report, whilst handling each of the issues in the template, should be structured on a thematic basis to make it easier for the intended audience to understand and act upon. This was useful for those with different roles in IdM. Additionally the Archive has its own record management approach, including templates for documents, and this is likely to be the case in many organisations.

- **Organisational size and context.** The Toolkit was created in the context of large F&HE institutions as a whole. The terminology reflects this. Any constituent part of a larger organisation wishing to use the Toolkit to test its own IdM should be aware that there will need to be some flexibility of approach recognising the size and complexity of the unit being reviewed. This is the case if only to take into account the IdM policy and procedures of the wider organisation.

3.4   *Immediate Impact*

The project has contributed to the examination of IdM and records management within the Archive in the context of the ISO27001 certification. As this project has focussed on the current state of IdM and potential improvements most of the impact will be seen in the future.

3.5   *Future Impact*

The work of this project will feed into the development of IdM and other policies and procedures within the Archive:

- Changes to registration and access arrangements for Archive managed resources;
- Production of a comprehensive user record policy for the Archive;
- Documentation preparation and review for continued ISO27001 certification and as part of the work supporting the Archive's activities surrounding the draft ISO 16363 for Trusted repository status;

- Review of the Archive's role as a provider of Shibboleth credentials through a virtual orphanage.
- Contribution – as far as this is within the Archive's ability – to education of users to enhance data and user information security.

By contributing to standards within the Archive all of the above will enhance the data services provided by the Archive to its primary stakeholders - data users and data creators/owners - and funders. The Archive will be in a better position to meet the requirements of those organisations funding social science resources not only within the UK but beyond, especially across Europe.

The case study output (with audit and gap analysis) is available through the project space on the JISC website (http://www.jisc.ac.uk/whatwedo/programmes/aim/ukdataarchive.aspx), the IdM Toolkit website (https://gabriel.lse.ac.uk/twiki/bin/view/Projects/IdMToolkit/WebHome) and the UKDAIM web page (http://www.data-archive.ac.uk/about/projects?id=2892). It provides other SPs and smaller institutions with an insight into the application of the Toolkit and some of the specific issues needing to be addressed for effective IdM. After 6 months the number of accesses and downloads of the project documentation, as well as feedback from users, will help to assess the impact and value of the project outputs. Where possible feedback will be sought directly from anyone known to have referred to this documentation, to demonstrate the benefits of this project.

4   Conclusions and recommendations

The main conclusion is that the Toolkit can be applied in the SP environment, though it would benefit from some modification to improve flexibility in its application and to recognise institutional variation. It is important that this modification work is carried out - under the auspices of JISC - to improve the usability of the Toolkit across F&HE. These issues will be fed into the Toolkit review scheduled for November 2011.

SPs using the Toolkit should focus not only on their internal processes, but also on the level of trust they put in any IdP whose users are seeking access to their resources. This has to be linked to any agreements, licences and contracts a SP has to deliver resources owned by a third party.

The critical reliance of SPs upon the IdM processes of IdPs emphasises the importance of:

- Increased use of the Toolkit to ensure effective and structured IdM across the F&HE sector in the UK;

- Clear guidance from the UKAMF on the approach UK F&HE IdPs should take in relation to authentication of users who have a non-UK or non-F&HE association with the IdP.

- Clear guidance available to data creators/owners about the level of granularity at which SPs can control access via the UKAMF authentication process, without further controls being applied by the SP itself.

- The relationship between IdPs and SPs, and the impact on service access. This should be a strategic priority for JISC to take forward when licensing content, with an emphasis on the easy reusability of model licences.

5   Implications for the future

The Archive will be taking forward the work of this project to improve its IdM policy and procedures. To assess the way in which the project was conducted and the usefulness of its outputs, a post-project review will be undertaken shortly after the conclusion of the project, in line with normal Archive practice.

All project outputs will be made available online and their use will be monitored. It is hoped that those who are using the Toolkit will find the specific experience of this project helpful, especially if conducting an assessment within a service environment. However, the usefulness of the Toolkit would be enhanced with some of the minor modifications mentioned above.

6 References

JISC Access and Identity Management Programme:
http://www.jisc.ac.uk/whatwedo/programmes/aim.aspx

Identity Management Toolkit Project:
http://www.jisc.ac.uk/whatwedo/programmes/aim/idmtoolkit.aspx

UK Access Management Federation for Education and Research
http://www.ukfederation.org.uk/

7   Appendix – IdM Implementation Issues

The Archive encountered two instances in which the authentication of users was affected by the IdM implementation at UK F&HE institutions.

7.1   AthensDA and recycling of user IDs (2007-2008)

AthensDA allowed users to access a range of resources using their normal institutional login credentials. The user did not need to worry about the associated Athens user identifier, and may not even have been aware of using Athens authentication.

For this to work the institution allocated an internal identifier - usually a 16 bit identifier - to each user within the institution. This unique identifier was passed to Athens and was permanently linked to a persistent user identifier (PUID). This PUID was relied upon by service and data providers to allow access by the user.

Where the user accessed a service which required registration and/or the acceptance of licence terms the user's acceptance was stored by Athens against the PUID. This meant that when the user attempted to access the service again the system checked the Athens profile and relied upon this to provide access. The aim was to ensure that a specific individual could be authenticated and allowed secure access to data, services and personal information.

In late 2007 it was discovered that institutional user identifiers were being internally recycled - that is, for example, allocated to a different user immediately after the departure of the original user from the institution - this did not break the link with the originally generated Athens PUID. Hence the new user and owner of this internal identifier inherited the access privileges and rights of the original user, without having to register or agree licences required by the service and data providers. The existing PUID gave the user illegitimate access to services, data and the personal information of the original user.

In dealing with this issue the Archive had to:

- Contact all F&HE institutions using AthensDA (and with users registered with the Archive) to ascertain their policy on recycling of identifiers;
- Force re-registration on users from any of these institutions which could not satisfy the Archive that the IdM policy would not cause the above problem. This affected nearly 7,000 registered users.

7.2   Shibboleth and duplication of user IDs (2008)

In late November 2008 a flaw was discovered in the operation of some institutional set-ups for federated access management (shibboleth) which could lead to unauthorised access to services and user personal data.

Where a user from an institution using shibboleth authentication registers with an Archive managed service the registration authentication system first checks that the institution has asserted user accountability. (This is a declaration made to the UK federation[1] by the IdP that certain user attributes will be assigned to a single user for their time with the institution, and will not be reassigned for at least 24 months after their last possible use in relation to that user).

The registration system then requires two attributes from the IdP:

eduPersonTargetedID - this identifies the user as a unique individual from a particular IdP. The format is a string up to 256 characters such as:

---

[1] The UK Access Management Federation for Education and Research, supported by JISC and Becta, and operated by JANET(UK). http://www.ukfederation.org.uk/.

SbuojhsD5enoss56@university.ac.uk

eduPersonScopedAffiliation - this provides details of the status of the user at the IdP. For the purposes of census the only acceptable statuses are member, faculty, student, staff or employee. Only users with these statuses are given access to resources.

The eduPersonTargetedID is stored in the registration database and thereafter provides a unique key to authenticate a user who wishes to access resources.

In November 2008 a user, contacted the registration help desk at the Archive regarding a complaint about a breach of confidentiality online.

He and another user at the same F&HE institution had been registering virtually simultaneously alongside each other at computers on the same network. This user completed registration, at which point the other user immediately had access to the complainant's personal details online without completing registration.

After internal checks and consultation with the institution it was found that it's shibboleth set-up was in some cases issuing null or non-unique eduPersonTargetedIDs.

It was discovered that an inconsistency between Microsoft's Active Directory service and Sun's Java system meant that identifiers intended to be unique might, in some circumstances, be re-assigned to different users. This could affect Shibboleth attributes such as eduPersonTargetedID, resulting in the possibility that two users might 'occasionally' be able to see each others' personal information held by SPs, or that institutions might have difficulty tracing the activities of individual users. This did not affect all institutions running shibboleth.

A fix was identified and the UK federation informed its members by email on 10 December 2008.

Where the fix was applied by an institution one consequence was that its users were assigned new eduPersonTargetedIDs. This meant that any user already registered would not be recognised as such when they attempted to access resources, meaning record matching or re-registration was required.