



Project Document Cover Sheet

Project Information			
Project Acronym	IDENTITYPROJECT		
Project Title	The Identity Project		
Start Date	1 November 2006	End Date	31 October 2007
Lead Institution	Cardiff University		
Project Director	Jean Sykes, LSE, Chair of Steering Committee		
Project Manager & contact details	Name: Joan Wright Address: Information Services, Cardiff University, 39-31 Park Place, Cardiff, CF10 3BB. tel: 029 2087 4496 fax: 029 2087 4285 email: wright@cardiff.ac.uk		
Partner Institutions	Cardiff University (CU), London School of Economics & Political Science (LSE), Birkbeck College (BBK), Goldsmiths College (GOLD), Imperial College London (ICL), Queen Mary University of London (QMUL), Royal Holloway College (RHUL), School of Oriental & African Studies (SOAS), University College London (UCL)		
Project Web URL	http://www.identity-project.info/		
Programme Name (and number)	<i>JISC E-Infrastructure Programme</i>		
Programme Manager	James Farnhill		

Document Name			
Document Title	Final Progress Reports		
Reporting Period	1 November 2006 – 31 October 2007		
Author(s) & project role	Joan Wright, Project Manager		
Date	7/11/2007	Filename	TidPFinalReport.pdf
URL			
Access	<input type="checkbox"/> Project and JISC internal		<input type="checkbox"/> General dissemination

Document History		
Version	Date	Comments
1.0	7/11/07	For comment by Steering Committee and submission to JISC
1.0a	9/11/07	Minor layout/spelling/grammar amendments



JISC Final Report

Table of Contents

Acknowledgements.....	2
Executive Summary	2
Background.....	3
Aims and Objectives.....	3
Methodology.....	3
Implementation.....	4
Outputs and Results.....	5
Outcomes.....	5
Conclusions.....	6
Implications.....	8
Recommendations.....	8
References.....	8

Acknowledgements

The Identity Project was funded by the JISC under the e-Infrastructure programme.

The project was led by Cardiff University and the London School of Economics & Political Science. The 10 partner institutions involved in the project were:

- Cardiff University (CU)
- London School of Economics & Political Science (LSE)
- Birkbeck College (BBK)
- Goldsmiths College (GOLD)
- Imperial College London (ICL)
- Queen Mary University of London (QMUL)
- Royal Holloway College (RHUL)
- School of Oriental & African Studies (SOAS)
- University College London (UCL)
- University of London (UoL, Associate Partner not funded by JISC)

We would like to acknowledge the help and assistance given by our JISC Programme Manager, James Farnhill, the Project Director, Jean Sykes, and the Key Researchers in each partner institution. We would also like to acknowledge the cooperation of the staff of our sister “ES-LOA” project.

Executive Summary

The broad aim of the project was to investigate and document the detailed Identity Management (IDM) situation in UK higher education, and to produce outputs to assist academic institutions in the UK wishing to take part in the newly emerging federated world in understanding what they need from their own IDM to enable this.

There were two major strands to the investigation:

- a broad survey of the current state of IDM in UK HE; 51 of the 184 UK HEIs responded plus 4 other organisations;
- in-depth audits of IDM practices at the 10 partner institutions.

These two major investigative work packages resulted in a great deal of raw data about the current state of IDM in UK HE. This raw data led to the project producing 7 reports, each of which may be viewed at the following URL: <http://www.identity-project.org/Findings.html>

A summary of the conclusions of all the reports is available at the following URL: <http://www.identity-project.org/Reports/AllWPCConclusions.pdf>

The experience gained through the 10 audits has been consolidated into a Research Guide which will be of value to other institutions wishing to evaluate their IDM systems or embark on an IDM project.

There is considerable demand for an IDM toolkit and guidelines. A follow-up project proposal is being developed which will be submitted to the Programme Manager for consideration.

Background

A key part of an access management federation is the trust between members that their respective Identity Management (IDM) arrangements are equivalent - or at least meet a minimum agreed level.

The JISC issued Circular 3/06, calling for projects to investigate e-Infrastructure Security, specifically (amongst other things) in the areas of Identity Management within Institutions and Identity Management across Institutional Boundaries. This led to the creation of The Identity Project.

It is important to note that the main outputs of The Identity Project are a series of reports, which are available from the URL given above, and thus this final project report is quite brief since there is no need to repeat their content.

Aims and Objectives

The broad aim of the project was to investigate and document the detailed IDM situation in UK higher education, and to produce outputs to assist academic institutions in the UK wishing to take part in the newly emerging federated world in understanding what they need from their own IDM to enable this.

The specific investigative methods stated in the project plan were:

- a comprehensive broad survey of the current state of IDM in UK academic institutions;
- a set of in-depth audits of IDM in a representative set of institutions.

Alongside the general investigation, the project also aimed to:

- investigate practice and policy around institutional membership;
- investigate how having NHS links affects an institution's requirements from IDM;
- investigate how having Grid Infrastructure affects an institution's requirements from IDM;
- identifying common problems (and their solutions if possible) apropos institutional IDM;
- examine current tools that assist with managing users, user groups and identities, and their applicability in an institutional context;
- attempt to establish community consensus on best practice in IDM;
- identify areas where further work is required.

Methodology

The investigation had two main strands:

1. In-depth audits of current IDM practices in the 10 partner institutions
2. A broad survey of UK institutions to see if this identified similar issues to those found in the in-depth audits

The methods used for these two strands are described in the next section.

The other work packages were based upon the findings of these two strands. The exception is work package 6, IDM Tools, which was conducted independently. The tools selected were those in widespread use in the UK academic community. The selection was checked against those referenced in the survey.

Implementation

Broad survey

In planning the broad survey, we considered:

- **Population to be surveyed.** Although the stated aim of the project was to investigate the IDM situation in UK higher education, we proposed to survey both HE and FE institutions. The inclusion of FE was not successful as only one such institution responded. This is thought to be because of the difficulty of identifying the relevant respondent in FE institutions, the length and complexity of the survey form and, possibly, lack of effort in FE institutions. The Steering Committee of 23 July 2007 took the decision to exclude FE from the scope of the survey.
- **Survey Design and Length.** The survey was designed by project staff. Drafts were extensively circulated to the Steering Committee, project partners and IDM specialists known to project staff and was piloted on some institutions. Their feedback led to several revisions. There is a balance between a short survey, which encourages response but finds out only minimal information, and a longer more informative survey which is likely to have a low response rate. We tried to strike the correct balance but in retrospect more rigorous pruning may have been advisable.
- **Survey Format.** Whilst an online survey was considered we decided to distribute it in Word format. This was because we felt that in most institutions it would require input from a number of people. The survey layout was designed so that it could be passed to different respondents and guidance was given in the table of contents and at the start of each section as to the type of role holder to which it was aimed. Feedback from respondents was mixed as to the preferred format. The survey was published on the project web site <http://www.angel.ac.uk/identity-project/Survey.doc>
- **Population frame and Distribution of survey.** The list of institutions to be surveyed was taken from <http://www.hero.ac.uk>. However these generally did not identify the appropriate person to which the survey should be sent. The Chair of UCISA, who is a member of the project Steering Committee, kindly agreed to send the survey out via the UCISA Directors mailing list. We also researched institutional web sites to find an appropriate addressee. The survey was publicised on a number of JISC mailing lists and was featured at 7 conferences and various JISC events.

The initial response to the survey was disappointing with only 22% of HE institutions responding by the end of June. The UCISA Chair contacted a number of institutions personally to encourage response. The selection was based on his personal knowledge of the institution and the gaps in coverage of the response to date. As a result the response rate was increased to 29% of HE. It was generally representative in terms of institution size and geographical location, with the exception of Northern Ireland from where no response was received.

Most respondents have either an IDM project underway or an IDM system in some state of operation and also viewed IDM as important now and likely to become more so. It is possible that institutions who have no IDM activity would be non-respondents.

In order to check the reliability of responses, visits were paid to 4 institutions for a more in-depth interview.

Institutional audits

Each institutional audit was performed by a Key Researcher (KR) seconded from existing institutional staff. Strong institutional support was regarded as essential. The process was overseen by an appropriate group or committee and a senior member of the institution who served on the project Steering Committee. The phases to the process were:

- **IDM Discovery** : to identify a comprehensive range of contacts to be interviewed and to discover official documentation. The original intention was that this would be topic-led. The KRs found it more practical for this to be person led – to identify those who carry out identity management, even if those individuals did not describe it in these terms. This was done by a combination of carefully-worded emails to staff, searching institution directories and direct contacts with obvious contacts such as MIS. This typically produced about 30+ candidates in

each institution. This was then reduced by applying a shorter list of 8 core IDM functions plus representatives of end-users.

- **IDM Investigation:** to schedule and carry out the interviews and record the data. A total of 116 interviews were conducted across the 10 institutions. The project team and KRs produced a list of topics to be addressed (these are listed in the Research Guide) but were not prescriptive about the precise wording of the questions. The typical interview length was about one hour. Unless the interviewee objected, digital recorders were used to capture the interview; this was very successful. KRs then transcribed the interview from the recordings and their notes onto the project Wiki. Audio files were also uploaded.
- **IDM Analysis:** to bring the findings into a final report. Some guidance on the structure of reports was given by the project team to ensure that they met the requirements of the project proposal. Otherwise KRs were given a free hand. Most followed the example structure adopted by the LSE report. Each report was signed off by the institution's Steering Committee member.

KRs met together with the project team 4 times to develop the audit process. There was very regular communication by email. KRs allocated 20% of their time (about 310 hours) to the project over the year. This was thought to be about right overall. However the IDM investigation phase was concentrated in a period of 3-4 months. There was a high workload in scheduling interviews with busy people towards the end of the academic year and conducting and transcribing lengthy interviews. If we were to repeat the project, we would aim to allow longer for this phase and to schedule it more carefully around the demands of the academic year.

Outputs and Results

The outputs of the project are the reports of each workpackage, in particular WP7 "Common Problems, Solutions, Best Practice and Future Development" and the guide for institutions wishing to conduct their own IDM audit. These have been approved by the project Steering Committee. They will be sent to the external stakeholders, such as MIMAS and EduServ, for their comments. All reports will be published on the project web site.

The original intention of the project was also to publish the institutional audit reports, at least to the UK academic community. Interviewees would be anonymised and institutions would have the opportunity to remove items that might compromise their security. However, it is not clear that this intention was clearly conveyed to all interviewees.

The project Steering Committee agreed that each institutional audit report was owned by the partner institution. The project would not publish these reports but would encourage the partners to do so after removing any material that might compromise their security.

Outcomes

Dissemination activities have shown that IDM is seen as of growing importance within HE but also as a difficult challenge where guidance is needed.

The Research Guide and the report on work package 7 will be of assistance to institutions wishing to evaluate their own IDM situation or planning an IDM project. A carefully carried out audit should enable an institution to:

- Discover any serious problems with existing procedures that need immediate fixing
- Know just how much identity management is carried out within the institution, with both qualitative and quantitative measures
- Identify tasks which are replicated unnecessarily within the institution
- Know which parts of the IDM within the institution are in a good and robust state
- Know where work would be required e.g. to meet the requirements for joining the UK Access Management Federation
- Evaluate the risks involved in moving to federated access management for external resources

The broad survey provides information on the current state of IDM in the UK HE community.

The report on IDM Tools will give guidance on the technical options to those planning or extending an IDM solution.

Conclusions

Each of the work packages undertaken produced its own set of conclusions. Some of these are reproduced here, to view them in full, however, they are available at the following URL:

<http://www.identity-project.org/Reports/AllWPCConclusions.pdf>

Broad Survey

Identity Management is an area with many aspects and potential areas that an institution can exploit to help them understand who its members are and track them throughout their lifecycle within the institution. Responses indicate that respondents have a very wide range of views about what Identity Management may consist of; however, the one common thread between respondents' views was centred on the area of account management. This account management thread is seen again when looking at existing IDM projects at respondents. Many respondents have some form of IDM project underway or IDM system in some state of operation, employ 2-3 FTE of staff effort on such projects. Over a third plan to spend capital between £50k and £100k on IDM in the next three years, whilst a further quarter plan to spend over £100k. However, such projects often seem somewhat limited in scope, mainly concentrating on the area of provisioning and deprovisioning of accounts. By and large respondents remained neutral when rating their IDM, partially because of this concentration on the one aspect of IDM.

Enhancing IDM within respondents generally seems to be a gradual process implementing parts of IDM at a time, rather than a one-time large IDM project that attempts to create a complete solution in one go. The projects often take existing institutional data and business processes and try to fit an IDM solution around them, rather than changing them to fit an IDM solution. On the other hand, respondents by and large expressed the view that they should be at least willing to change some business processes if it would enhance their IDM.

All of this information leads to a few key conclusions about issues institutions may face. The first conclusion is that before an institution embarks upon an IDM project, they probably need to first agree on what they mean by "Identity Management", given the wide range of views that permeate an institution. Secondly, when institutions are implementing IDM, the fact that generally implementation is done as a gradual process using existing institutional data and business processes means that the key issues institutions will face will be centred around the area of the quality of the existing data and processes: Just because data and processes are good enough for the corporate system in which the data resides does not necessarily mean they are good (and timely) enough for an IDM solution - which may make different demands of them. Additionally, when integrating several existing systems via an IDM system, institutions may find that issues such as inconsistency in data definitions between systems and duplication of data swiftly become issues that need addressing. There are two approaches to use to deal with these last two issues – either to attempt to solve the data issues before implementing IDM, or to rely on the implementation of IDM to expose such issues and thus create the pressure to resolve them.

Membership

The conclusions to WP3 are a set of principles which are worth bearing in mind when planning identity management activities.

- *User Categories* - HEI membership is much more complex than a naive analysis would suggest, and there many more categories than envisaged by (say) the eduPerson schema, with different rights. Not only that, but even apparently well understood terms such as "student" and "staff" are more fuzzy than might be expected. The precise definitions of these differ between HEIs, but more homogeneity of definition is likely to be required by licensing in the future.
- *Credential Management* - Automated processes used for common categories of users appear to work well and securely. Some departments may, however, act independently from the

central administration processes, which can lead to problems with integration of data about department members with the rest of the institution.

- *Attribute stores* - HEIs contain large numbers of attribute stores of various kinds which are used for different purposes. These have complex interrelationships which need to be managed carefully to avoid duplication of effort and insecure methods for transferring data.
- *Unique Identifiers* - Many institutions found that a universal unique identifier for individuals worked well for synchronising data from different sources and for resolving issues with users who have multiple relationships with an institution.
- *User understanding* - Users are generally not greatly concerned or knowledgeable about the ways in which data held by the institution about them is used. This seems likely to change if there are scandals about data exposure in UK HE, and through the advent of federated access management.
- *Atypical individuals* (individuals whose relationship to the institution is other than staff and students, and even those categories when their relationship proceeds down a non-standard route) - These are usually handled outside the main identity management processes of an institution, both in terms of business processes and technical solutions. Ad hoc processes can lead to difficulties in accountability and security. Some particularly troublesome groups include users with NHS links, contractors, temps and employees of third party suppliers
- *Prior identity discovery* - Most institutions carry out some form of prior identity discovery, but this is usually limited to simple automated procedures or responses to users volunteering information about a previous relationship to the institution, due to the difficulty of the problem and the time it takes to carry out manual checks. The limits of the process indicate that systems that manage identities need to be able to merge identities discovered to be duplicated.
- *Virtual Organisations* - Currently, identity management for virtual organisations is carried out in an ad hoc manner. This is likely to change, with Shibboleth being singled out as a key technology for this area.

IDM and the NHS

Institutions with links to the NHS may encounter several extra IDM issues that they may have to deal with. These centre around additional membership issues, the lack of data authority to provide an IDM system with identity information about NHS staff, the need to use NHS and institutional networks, library access, electronic resources, and physical access. Some institutions with such issues have enacted very similar solutions to the issues, however, many issues remain unsolved by all.

IDM and Grid

The main identity management challenge for enabling grid computing is to make registration of external users lightweight. To do this, the grid should be adapted to take advantage of the identity checks already in place for organisation identity management systems. The cost of identifying users is high and hence unscalable using the current CA methods. However, organisations put some effort into identifying staff and students at the beginning of their employment or studies.

Combining the grid identity management with the organisation's own checking would provide a scalable method for establishing identity. The recommended method for doing this would be for each organisation to host its own CA and sign certificates for their local users. Running a CA has proved to be a time-consuming operation in its own right. However, by automating the issuance of certificates through the local identity management system, this need not be the case.

Private and public keys can automatically be created for each user when they are entered into the organisation's identity management system. The user can then retrieve a grid proxy certificate through a server (such as a modified MyProxy server).

In order to make organisational CA certificates acceptable to other sites, a UK PMA should be created to provide a consortium of organisations that meet a specified standard for issuance of these certificates, and to lobby for the inclusion of their CA certificates into appropriate grids such as the NGS.

Implications

The project showed that institutions are looking for best practice guidelines and toolkits for IDM. Tim Phillips (Bristol/RUGIT) put to the Steering Committee a draft proposal for a follow-up project to define an IDM toolkit and roadmap. This is being developed for submission to JISC,

Recommendations

Universities and colleges are very large and complex organisations. Generally the IDM fits the purpose it serves and adheres to statutory requirements. In order for the organisations to develop further in the area of IDM the following issues should be addressed:

- improved documentation and standards – each organisation should develop, implement and maintain their own IDM standards, policies and procedures. These standards and documentation should encompass both centrally managed IDM systems as well peripheral and satellite systems that exist in departments that are maintained semi-independently from central systems. It is acknowledged that a complete centralisation and integration is not feasible; however, coordination can be improved;
- improved awareness – to achieve improved management and coordination of administrators there should be more IDM training available; the improved awareness together with consistent standard and documentation should result in higher IDM level of service across universities and colleges.
- introduction of regular audits – to ensure an appropriate quality of IDM documentation and standards, and also IDM awareness amongst the staff, each institution should set up a regular audit process. The precise form of this process should be up to each individual institution, for example it may be carried out by a separately formed unit or a group of professionals seconded from other units. It should be noted that an IDM audit unit has to have sufficient standing within the institution so its recommendations are implemented institution wide.

The introduction of an IDM audit unit addresses some issues uncovered in the course of this Institutional Audit Case Study: groups' autonomy, heterogeneity and lack of central IDM administration. Whilst it seems rather impractical, or even impossible, to completely integrate and unify IDM administration, an IDM audit unit should be instrumental in creating a semi-integrated IDM environment.

The audit units should be guided by the ISO 27001 (previously ISO 17799) standard and also take an overall responsibility of an institution's adherence to them. A useful guide is available at <http://www.ucisa.ac.uk/ist/>

Better documentation and standards, combined with high level training, monitored and sustained by regular audits should create a good foundation for federated access implementation projects.

References

N/A