

Conclusions of TIdP WP Reports

This document brings together the conclusions of each of The Identity Project's 7 work packages.

WP1 - Broad Survey

The Identity Project's Identity Management survey constituted a survey of the UK's 184 Higher Education Institutes (HEIs), of which 28% actually took part. These institutions were fairly well representative of the community as a whole in terms of geographical location (with one exception), size, and institutional affiliation. The responses to the survey indicated that the vast majority of respondents see Identity Management as an area currently fairly important to them, and an area whose importance will increase in the future.

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.

WP2 - Audits

The final report on WP2 concentrates on the process of the audits, as developed by the project and as it may be re-used by other HEIs. As such, it does not contain conclusions and recommendations. However, the conclusions of the individual audits at partner institutions form a major part of the

reports to WP3-5 and WP7, particularly WP3 and WP7 which rely more on the audits than the survey.

WP3 - 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.

WP4 - 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.

WP5 - IDM and the NGS

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 MyProxy1?? 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.

WP6 - Technologies for IDM

Organisation wanting internal Identity management

Consider packaged product such as Novell Identity Manager, Sun One Identity Manager, Microsoft IIS (Identity Integration Server) and Oracle Identity Manager. These may require serious commitment to a wider suite of products to deliver real value. Also consider their suitability as point solutions, supplemented by existing or new applications and processes. Use of standards, such as DSML and SAML will assist in interoperability.

For an open source solution, keep an eye on Bandit.

Organisation wanting to be a Shibboleth IDP

Use of the official Shibboleth software should be considered, although it has been implemented independently (e.g. Guanxi at <http://www.guanxi.uhi.ac.uk/index.php/Guanxi>).

An authoritative authentication provider will be required for a Shibboleth implementation. You can have more than one authentication provider, but duplication across many leads to problems (such as: which username/password should a user who exists in more than one use?). If you don't already have a consolidated one in directory or database form, then consider using the Penrose directory to present a virtual view of various providers. Also consider synchronising the various providers into a single repository using an a product from a major vendor (as listed above). Penrose is likely to offer quick wins, but the latter may be more reliable, but take longer to implement. For this reason, Penrose may be suitable as a proof-of-concept.

You will also need a single source of attributes about people who have authenticated. This can be in the form of a single database or directory.

If complex authorisation policies are required, consider the use of Grouper, Signet or Permis.

Service provider wanting to be FAM compliant

Consider whether to implement a consolidated solution which closely integrates service provider with identity provider, versus a modular solution which emphasises interoperability. Consider Permis as the core authorisation engine. Consider standardisation on standard protocols in widespread use – Shibboleth for the educational community, or SAML for more widespread use and support in packaged products.

Set of organisations wanting to start a federation

Consider where the products and projects appear to be converging. At the moment SAML (or a subset of it with Shibboleth) appears the best bet for “managed” federations, and OpenID? for more informal federations.

WP7 - Common Problems, Solutions, Best Practice and Future Developments

The conclusions to WP7 are a set of recommendations for Universities and Colleges. In order for the organisations to develop further in the area of IDM the following issues should be addressed:

- improved documentation and procedures - each organisation should develop, implement and maintain their own IDM standards, policies and procedures. These, together with documentation, should encompass both centrally managed IDM systems as well peripheral and satellite systems that exist in departments and are maintain semi-independently from central systems. It is acknowledged that 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 an improved IDM's level of service across universities and colleges.
- introduction of regular audits - to ensure an appropriate quality of IDM documentation and standards, and also the level of 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 separate unit or 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 by all responsible of IDM. The introduction of an IDM audit unit addresses a good number of issues uncovered in the course of this Case Study and referred to earlier in this report: groups' autonomy, heterogeneity and lack of central IDM administration. Whilst it seems rather impractical or even impossible to completely integrate and unify IDM administration, the IDM audit unit should be instrumental in creating a semi-integrated IDM environment. The audit units should be guided by the ISO 27001 standard and also take overall responsibility of an institution's adherence to the standard.

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