The Identity Project[1]

Work Package 2: In-Depth Case Studies of Identity Management

UCL Final Report

Margaret Stone
IT Services Development Officer, UCL Library Services

This report presents the results of an audit of identity management practices at UCL, as part of Work Package 2 of The Identity Project.

After an introduction to the organisational context and a description of the audit methodology, the results of fifteen interviews are presented thematically. Throughout the text, information arising from the interviews is referred to by letter, eg. (A). These references are expanded in the Appendix.

Please note that this published version of this document has been edited to remove pieces of information which might compromise UCL's identity security processes.

[1] http://www.identity-project.info

Glossary

Departmental Administrator
Member of staff in a UCL department having human resources responsibility.

Federated access management (FAM)
Management of access to resources through a trusted common set of policies and rules amongst a group ("federation") to aid cross-domain authentication and authorisation. The main UK organisation is the UK Access Management Federation[2].

Grid computing
Colloquial term for distributed computing: large-scale computing consisting of multiple nodes, especially the UK National Grid Service[3]. See also **research computing**.

IdM
Abbreviation used in this report for Identity Management.

Information Systems (IS)
UCL's central computing service, which provides user accounts for staff, students and certain affiliates. The "IS username and password" will in future be known as the "UCL username and password".

Key Researcher
The researcher appointed by each partner institution in the Identity Project to carry out the institutional audit.

Management Systems
UCL Management Systems Department, responsible for the development, installation, maintenance and support of corporate systems including HR, Registry and Finance.

Moodle
An open-source Virtual Learning Environment (VLE), which is UCL's supported VLE from summer 2007, replacing WebCT.

Research computing
Computing services for the support of research, especially **grid computing** or distributed computing. When capitalised, the name of the support team for this service, UCL Research Computing.

Services System
UCL's in-house Oracle-based system for managing access to various services for UCL visitors (non-staff and non-students).

Shibboleth[4]
An open-source architecture and toolset for identity management within **federated access management**.

UPI
UCL Person Identifier, a unique identifier assigned to every individual who has a bona fide association with UCL, and used as the key to person data for this individual in all corporate support systems.

VLE
Virtual Learning Environment, a software system to facilitate online learning and course support.

[2] www.ukfederation.org.uk
[3] www.grid-support.ac.uk
[4] shibboleth.internet2.edu

1 UCL and identity management

1.1 UCL in context

Founded in 1826, UCL is London's leading multi-faculty University, and one of the most consistently highly-ranked research institutions in the UK after Oxford and Cambridge. The Government's 2001 Research Assessment Exercise awarded top marks of 5 or 5* to 58 UCL Departments. UCL has a particular strength in clinical and pre-clinical studies: UCL has one of the largest Medical Schools in Europe, based on three campuses. All UCL medical libraries are currently joint libraries, serving both Higher Education and NHS users.

UCL research and teaching are carried out by more than 4,000 academic and research staff based in 72 academic departments. In terms of student numbers, UCL has seen a steady growth during the last decade to 19,365 in the academic year 2006-07 (11,930 undergraduate and 7,435 postgraduate). Additionally, UCL employs over 1,000 administrative staff.

UCL, therefore, has a substantial number of identity holders, requiring access to a highly diverse portfolio of systems and services. Local computing applications protected by some level of authentication include desktop and email services, a Virtual Learning Environment (VLE), diary software, the UCL intranet, and a number of other internal applications housed in different administrative departments (Human Resources system, Registry (student record) system, finance system, etc). A joint identity/access/library card has recently been introduced and the buildings access system is being extended. Beyond this, UCL also manages authenticated access to online learning and research resources through UCL Library Services, including over 9,000 electronic journals, around 200 subscription databases and increasing numbers of electronic books.

1.2 Identity management at UCL

UCL is quite advanced in terms of identity management, but less so in access management.
Some of the challenges which UCL has enumerated in terms of identifying individuals associated with the institution include:

- People change department during their time at UCL;
- People straddle more than one department at the same time;
- People change status: undergraduates become postgraduates; students graduate and become staff;
- Dual roles: many students do paid work for UCL;
- Many staff register for higher degrees and are therefore also students;
- Many people have “loose association with UCL”, eg. they are neither on the payroll nor enrolled as students;
- UCL has associations with the NHS which increase the complexity of identity management.

In order to tackle these issues at UCL, a set of processes involving Human Resources, Registry and departmental offices is used to assign an identifier called UPI[5] (UCL Person Identifier) which is unique to every individual who is, or has been, a member of UCL and requires access to resources. The assignment processes are mainly through the Registry and Human Resources (primary systems) but because there are so many individuals with shorter term associations ("visitors") there is a third primary system called the "Services System". The Services System was built in-house and is being rolled out to all departments from July 2007. Typically Departmental Administrators are authorised to use the Services System, as they are the staff members most likely to know whether granting access to resources for a visitor is appropriate or not.

[5] www.ucl.ac.uk/upi

UCL's recent Replacement Access Library and ID card project (RALIC) is an example of coherent identity management which ties together digitised photographic identity, building access and library access in a single card. It is reliant on the UPI processes to establish and assign identity as a pre-requisite to issuing the card, and UPI has a technical index to tie these different systems together.

UPI also has some knowledge of the different groups that people are in i.e. staff, student, department, visitor, but does not know about roles (e.g. Head of Department) and does not know about states within a role (paid fees/not paid fees).

At UCL there is a strategic drive towards single sign-on - i.e. using the same authentication credentials (username and password) to access a variety of electronic resources. In practice, this is "synchronised sign-on" in a heterogeneous environment of different computer systems with different authentication standards. Password changing is done through a web form which can enforce a common standard in password choice across all platforms, and once the new password is chosen it is "fed" to each system separately.

2 Audit methodology

2.1 Identifying key Identity Management topics and stakeholders

In accordance with the project guidelines, a local project board was formed at UCL to oversee the audit process. There was no appropriate existing body at UCL, so a group was formed of the Director of Information Systems, a member of the Library Services senior management team, a project manager from Management Systems, and the co-ordinator of research computing at UCL, along with the UCL Key Researcher for the project. This board met six times during the project and its early meetings focused on establishing the key areas of Identity Management (IdM) which were of interest to UCL, and the key stakeholders and practitioners in IdM.

The board began by considering the topic list from the project deliverables, to identify the UCL stakeholders in each area. From this, the Key Researcher produced a list of suggested individuals, supplemented by the results of a trawl of the UCL website A-Z index (which includes all central departments and functions). This was taken back to the project board and refined following further comments. At this stage, the list was as comprehensive as possible. It included some specific departments which were believed to have particularly noteworthy IdM needs or practices, but this only included those known to the board members.

2.2 Identifying other Identity Management practitioners

In order to broaden the list of potential interviewees beyond the current knowledge of the local project board, an email was sent to the "all-staff" email list at UCL. It was sent by the Key Researcher, but from a "Reply-to" address of identity-project@ucl.ac.uk, and co-signed by the Director of Information Systems (chair of the local project board) to lend as much weight as possible to the request for information. Based on guidelines from the central project team, the email simply asked staff if they could answer "yes" to two questions:

As part of your work, do you:

1. ask anyone to prove who they are?
   or
2. maintain information about individuals which is used by them to gain access to electronic or physical resources?

The aim was to prompt response from individual staff members who were involved in any way with identity management, including areas which the researchers may not have considered. Responses would be filtered and prioritised later. The email also provided background information and provenance for the project, and then asked respondents to indicate how their work covered the areas above, advising them that a questionnaire would be sent to them for

full details. It also attempted to provide an incentive for respondents, stating that "By filling in the questionnaire, you will have the opportunity to inform decisions which aim to make managing identities and access more efficient, and potentially make this area of your work easier."

The all-staff email elicited 30 responses, of which around half were added to the long list of potential interviewees, which grew to 50 roles or areas for investigation. The others showed evidence either of "trivial" IdM or of being covered by other roles on the list.

2.3 Prioritising interviewees for the audit

Key Researchers from all the project partners met together to establish joint priorities for choosing interviewees. All institutions had uncovered many more stakeholders and practitioners than there was time to interview, so prioritisation was essential. It was also decided to have a common core of interview areas, to facilitate comparison between institutions. Beyond the core list of 11 topics, because of time constraints, UCL was able to add only four further interviewees from the long list described above. These were in the areas of NHS and Grid computing (relating to the project work packages), management systems (at the core of UCL's existing central identity management practices) and records management / data protection. Other stakeholders would be followed up by email as time permitted.

2.4 Arranging interviews

For each of the 15 proposed interview topics, an individual staff member was identified and a personal email was composed, drawing on a template outlining the project (it was not assumed that these interviewees had read the all-staff email). The email highlighted the area of the person's work which was of particular interest to the project, and invited them to agree to an interview or to nominate a more appropriate colleague if necessary. In most cases, the interview was arranged by email, but telephone follow-up was used where a response was not received within a week. Despite the Key Researcher being personally unknown to many of the interviewees, many of whom were senior managers, the speed of response and acceptance rate were pleasing, and only minimal follow-up was required.

Interviewees were drawn from the following functional areas:

- Access Systems
- Alumni Relations
- Records Office
- Financial Systems
- Human Resource Operations
- Information Systems
- Learning Technology
- Library Services (Membership Services and NHS links)
- Management Systems
- Registry
- Research Computing

plus one member representing each of the following user communities:

- Academic Staff
- Administrative Staff
- Student

2.5 Interview topics and methodology

The project partners collaborated to produce guidelines for questioning in the interviews. It was agreed that partners would adapt the template to their own needs, and have the freedom to adapt the questions to the interviewee, and UCL made significant use of this freedom. The Key Researcher found that the flow of conversation always lent itself better to an informal discussion, ensuring that key concepts were covered but following up points as they were raised by the interviewee.

The interview templates covered technical issues, business process issues, and unmet requirements. Interviewees' responsibilities often covered both technical and process aspects of IdM, and all were asked about IdM requirements which were not being met by existing systems. The templates attempted to describe IdM in "layman's terms", but the Key Researcher found that quite a lot of additional explanation was required for the context of each interviewee.

Shortly before each interview, a further email was sent to the interviewee, partly as a reminder, but also including some guidelines to help them to prepare and to manage expectations. Topic areas were listed in advance, but not specific questions.

Each interview lasted no longer than an hour, for the benefit of scheduling, concentration spans and post-processing. The interviews were recorded (except where the interviewee preferred not), but notes were also taken and the recordings were used only by the Key Researcher to clarify any uncertainties in writing up the notes.

2.6 Additional questionnaires

Because of the limited number of interviews which were possible, brief questionnaires were also emailed to those who had responded to the all-staff email and were on the "long list", and to one or two other key stakeholders from the long list. However, as expected without any personal follow-up, these questionnaires produced little fruit. Seven brief replies were received. In each of these cases, further questioning would have been desirable in order to uncover further some interesting IdM practices, but time was not available for this.

The following topic overviews are therefore drawn from 15 interviews and other email contributions.

3 Credential management

3.1 Credentials in use at UCL

The types of credential available to members UCL by virtue of their membership include:

- Information Systems username and password
- UCL identity card, including library borrowing and buildings access
- Departmental computer username and password (where available)
- ADS (Administrative Desktop Service) username and password
- Various usernames and passwords for local systems
- Various local access keycodes and keys

3.2 Issuing of credentials

The Information Systems (IS) username and password form the lynchpin of access to electronic services at UCL. These are allocated automatically by IS for all students and staff (J), based on the individual's entry in one of UCL's primary systems and the allocation of a

UPI. This requires an accurate synchronisation between the entry and activation of the primary record and the need for an IS account.

Given the centrality at UCL of IS accounts, it is of course important to keep an eye on the range of "other" accounts, beyond the standard staff and students which make up the bulk. This includes "visitor" accounts, which can have significant staff-level access rights and are currently requested by paper form, signed by departmental computer reps. There are also "role" accounts, which are tied to a role (single or multiple users), requested by computer reps and allocated to a responsible person, who may or may not be a user of the account.

The Administrative Desktop Service (ADS) username and password provide access to a historically separate Windows desktop, including email and filestores, for around 700 UCL staff in a range of administrative departments, including Human Resources, Registry and Finance. These credentials are authorised by the departmental computer rep and issued by Management Systems department, and are not yet synchronised with the IS password (though the username is manually created to be the same), but this is planned (W).

The UCL identity card is also allocated automatically by association with the primary systems (D), for staff, students and visitors. The new card, which was introduced recently, will become increasingly important as UCL plans to add access control to more and more buildings. Once the Services System (I) is live, no person records will be created manually on the system.

3.3 Expiry of credentials

The practice of expiry or deletion of accounts varies between IS accounts and ID cards.

In the primary systems, students have an expected end date (the official HESA[6] end date), which is updated if their circumstances change (H), whilst staff records expire when the post to which they are attached ceases to be funded - this may be fixed-term or through resignation (C). Student ID cards expire as soon as they reach their end date (D). Staff ID cards have a ten-year validity, regardless of temporary or permanent contract, and expire when the person is recorded in the HR system as having finished (D).

3.4 Re-use of credentials

UPIs are never re-used (I), so that a user can have a long-standing association with UCL in as many different incarnations as are required. IS usernames for undergraduates are never re-used, while the policy for staff and postgraduates is under continuous review.

3.5 Certificate management at UCL

Personal certificates are not used for access to central systems and services at UCL.

UCL provides guidance[7] for researchers on applying for a UK e-Science certificate, and the services of a Registration Authority to obtain the certificate. These certificates are then managed manually by the registered owner.

[6] www.hesa.ac.uk
[7] www.ucl.ac.uk/research-computing/services/certification

4 Attribute stores and usage at UCL

4.1 Storage of attributes

Person data at UCL is distributed across a range of systems, but large amounts of the data held about each person can be retrieved using the linkages of the UPI (I).

The primary data source for each person is the HR system, Registry system, or Services System, for staff, students and visitors respectively.

According to the UPI team,

> "The UPI code acts as a key so that personal information in central systems can be tied together and updated. This means that accurate personal information can be transferred between systems without relying on separate data being stored in several different locations. It also allows data to be readily updated - e.g. if an e-mail address or phone number is changed, this can be passed to Human Resources or the Registry automatically."

No particular metadata standards are used for person data. One interviewee (B) commented on the multiplicity of standards which exist, for example for personal names and addresses, and the need to conform to data formats and validations of the various database systems in use.

Various methods are used for updating attributes. In the primary systems, most attributes are updated manually by authorised staff, although limited self-service options exist for the Registry and HR systems (C, H). For secondary systems, some attributes are updated automatically from the primary systems. For example, in the Library system, email and postal addresses are updated automatically from the Registry and HR systems, but other updates are processed manually, though some alerts are provided automatically (N). In the case of IS accounts, whilst student statuses and departmental affiliations are updated automatically from the Registry system, staff IS accounts are not automatically updated. If a staff member changes departments, a new account is created and the old one deleted, because of the link between departmental affiliation and the user ID itself (J).

Attributes which are local to the secondary system are also updated through a mixture of central management and self-service. For example, changes to user records on the financial system are all handled by processing paper forms (B), whilst users of the Moodle VLE can update aspects of their data (M).

This complex map of updating procedures presents a challenge for change control of attributes. System owners and administrators need to have an up to date picture of which attributes need to be updated from another system, and of the effect that updating a particular attribute may have in other systems (X).

4.2 Usage of attributes

One of the difficulties with such a system of distributed data storage and management is that those responsible for the creation of data are not necessarily those with an interest in the use of particular attributes. For example, the data required for alumni relations may not be of direct relevance to those involved with managing current students, but the alumni system takes all its data from the Registry system (K).

Attribute usage has implications for the amount of personal data stored by each system. One interviewee (E) was particularly concerned that no system should gather more information about them than was necessary for the functioning of the institution, in order to minimise the "Big Brother" scenario. The Alumni Relations office (K) produced a specification of which

student attributes were required to be transferred from the Registry system. The future addition of student photos to the Registry system (H) requires careful specification about the usage of this particular attribute. The whole area of attribute usage could be a topic for further study: to examine attribute requirements across systems and eliminate redundancy.

4.3 Access management

A major use of person attributes is to control access to systems. This is an area which UCL plans to investigate centrally as part of its current Information Strategy Implementation Plan[8], with a view to joining up current access management procedures. Defining roles and user groups based on person attributes is a complex and challenging task, and requires common agreement on attribute definitions (eg “staff”, “visitor”, etc.) (X). Some current examples of attribute use for access management follow.

- Attributes from the primary systems are used, via the UPI system, to add IS usernames to various permission files for the UCL intranet (I). These are also used for mailing lists, including those for individuals with more "casual" associations with UCL, and for access to electronic library resources (N).

- UCL staff are assigned to a range of pre-defined roles within the HR system (C), such as Heads of Department and Departmental Administrators, who are then able to access certain HR functions by this authorisation.

It might in theory be possible to define a sufficient number of person attributes in primary systems to map to authorisation rules in secondary systems, but one interviewee (B) commented particularly on the challenges of such centrally-defined roles and authorisation rules. It was felt that upgrades to systems would continually necessitate re-definition of the mappings between any central attributes and the authorisation rules of the secondary systems, and that this would be a very complex problem.

The distributed responsibility for access management to many systems at UCL adds another challenge. For example, with access to electronic library resources, Library Services is responsible for the user interface, Information Systems provides the authentication and authorisation infrastructure, whilst Management Systems controls the mechanism for feeding person attributes from the primary systems (X).

4.4 Attributes for federated access management

UCL is starting to make more use of its person data for federated access management (FAM), using Shibboleth. The existing directory is able to supply the minimum attributes recommended by the UK Access Management Federation [9] (known as eduPersonPrincipalName, eduPersonScopedAffiliation and eduPersonTargetedID) but further work will be required at UCL in order to comply with any specific data requirements by individual service providers, and to take advantage of granular access rights based on person attributes which are not already present in the basic directory data at UCL.

The main area of application of FAM at UCL so far has been access to electronic library resources (N). However, the audit highlighted several other potential uses for FAM, including access to the VLE (M), and to research computing facilities (A), and to a remotely-hosted database for research administration (P). Each of these, and other, uses would require sufficiently granular person attributes for authorisation.

[8] www.ucl.ac.uk/isip
[9] www.ukfederation.org.uk

5 Affiliate identity management

5.1 Classes of non-standard user

Examples of groups of users who are entitled to use UCL services but are not staff or students include:

- Honorary staff - teachers and researchers associated with a UCL department, including NHS staff teaching in the UCL medical school (J,O)
- Affiliate academics - academics from overseas who wish to spend a period at UCL, normally between four weeks and 12 months, pursuing their own research either individually or in association with UCL staff. Scheme[10] administered by UCL Human Resources.
- Departmental visitors - anyone who is temporarily associated with a UCL department, on a more ad hoc basis than the above categories (I,J).
- Library users - a whole range of categories, listed on the Library Services membership web pages[11] (N)
- Research computing users - researchers collaborating with UCL academics and requiring access to UCL's research computing facilities (A)
- Summer school and other short-course students – (including professional development) ranging from one day to several weeks, who may require access to computing facilities (J)
- Conference guests - who may require access to computing facilities, via UCL clusters or wireless network (J)
- Guests in UCL Halls of Residence - who can access the internet via UCL's network (J)
- Non-UCL students on collaborative courses - who may require access to course content created by a UCL teacher on the UCL VLE (M)
- UCL alumni - who are entitled to certain tailored services, and to library membership (K)
- Retired UCL staff - who are entitled to access certain electronic library resources under new licence terms (N)

5.2 Handling non-standard users

Honorary staff and affiliate academics are entered in the HR system. Departmental visitors will be handled by the new Services System. Library users who are not covered by the Services System are entered manually on the Library system.

Areas of potential difficulty include:

Appropriate authorisation for non-standard Information Systems accounts
In addition to e-resource access, there are other uses for non-standard (or “lightweight”, no disk quota) IS accounts, including access to the VLE only, or access to the internet for non-UCL users of halls of residence. It might be possible to configure more granular authorisation for IS accounts, so that users only have access to the services they need or to which they are entitled.

Access to UCL systems for collaborating learners and researchers
At present, learners and researchers who are involved in collaborations with UCL have their own accounts on the relevant UCL systems (eg. the VLE (M) or research computing facilities (A)). These are created and maintained manually, and require rigorous procedures for initial authorisation and for revocation of access. Federated access management could be of use here, where the identities would be managed by the home institution and access managed by trust agreements.

[10] www.ucl.ac.uk/hr/docs/affiliate_academic_scheme.php
[11] www.ucl.ac.uk/Library/joining.shtml

5.3 Personal data gathered for research

A significant area of identity management at UCL is the gathering of personal data as part of research projects. In most cases, the individuals being managed are not UCL members. This is a major area of work for the Records Office (F), which provides guidance on the management of personal data, and co-ordinates compliance with UCL's Data Protection Registration.

The individuals whose data is held in the course of research do not necessarily have access to UCL facilities, nor any ongoing association with the institution but, if an overall picture of institutional identity management is pursued, these databases should perhaps be included.

6 Prior ID discovery

6.1 Mechanism for prior ID discovery

The UPI system at UCL is intended to facilitate links between all possible records for any one individual associated with UCL (I). If a person is both staff and student at the same time, for example students who work part-time in the library, their multiple records are attached to the same UPI. Since the UPI is allocated for life, a user can study at UCL, leave, and then return many years later but still have their records connected via the same UPI. All the other attributes associated with a person may change.

On the primary UCL systems, records are not deleted but rather made inactive. This means that linkages are maintained and that records can be reactivated if the user returns to UCL.

6.2 Problems with prior ID discovery

When a person record is being entered on a primary system, the record creator must confirm whether or not there is a pre-existing entry for that user and if there is more than one possible candidate they must choose the correct match.

This system only covers those who have a UPI - those who have had records on at least one of the HR, Registry and Services Systems. Even when the Services System goes live, there will be a phased adoption by departments and by services, and there may remain a few types of affiliation with UCL for which there are currently no plans to use it (eg. library visitors and users of the VLE only). There are also historic records where the UPI linkages are incomplete (K) and these could only be addressed by a retrospective conversion project.

If an undergraduate student returns as a postgraduate student, a new user account and email address are automatically assigned to them. They can optionally choose to allocate their previous email alias to their new address (and to transfer files from the old account to the new) but this does not happen automatically.

If a student also becomes a staff member, staff privileges can be added to their existing student account and their existing email address can be added to the correct UCL mailing lists (G). They will however automatically receive an additional IS account and email address, which they will have to manage separately if they wish to use them.

The need for the UPI system is demonstrated in examples such as that of the alumni system (K). This has regular checks for duplicate records built into it, as some students have previously studied at UCL on one or more occasions. Where a UPI is known for that student, it is easy to avoid duplicating records, but there are still many historic records which do not have UPI data.

7 Identity security and privacy

Risks surrounding identity management include the potential for unauthorised access to a person's data, the potential for incorrect attributes or access rights to be assigned to an individual, and the potential for a user to assume a false identity for illegitimate or harmful purposes.

These may be related to the storage, transport or release of personal information.

8 Requirements for use of credentials

Historically, individual applications requiring the use of identity management credentials at UCL have been scoped and implemented independently or within groups of applications which share a common management responsibility. The introduction of UPI has facilitated greater links and has had an impact on specifications, and the strategic drive towards synchronised sign-on will continue this trend.

8.1 Synchronised sign-on

UCL's policy is to synchronise usernames and passwords wherever possible with the IS username and password. This is synchronised sign-on, rather than single sign-on, as the user has to log in to each system separately, but they have a single username, and password changes are synchronised by interactions between the systems.

Some systems (usually those which are smaller scale) do not form part of this synchronisation. For example, usernames and passwords for the research computing facilities (A) are managed separately. A large system which does not use the central UCL username is the library borrowing system, which is based on the barcode technology used to issue books (N). The financial system is also not yet synchronised with the central username. The interface to the Alumni Web Community is a mixed economy of UCL username for current students (limited functionality) and a separate username and password system for alumni (K).

Some departmental computer networks are also synchronised with the central username and password. Many are not, but are progressing in this direction.

8.2 Implications for credential use

A recent example of the influence of the drive to single sign-on is the use of institutional usernames and passwords for federated access to electronic library resources. This required compliance of UCL's directory and processes with the specifications of an external body (the UK Access Management Federation), and any further developments of the directory now have to take this usage into account. In addition, the fact that a wide range of UCL users are eligible for credentials for external electronic library resources has implications for existing credential allocation policies internal to UCL. A joined-up approach to such policies will continue to become increasingly important.

9 Virtual Organisations and Research Computing

9.1 Research computing at UCL

UCL has a network of bodies to oversee its research computing activities, with a co-ordinating manager[12]. UCL does not currently contribute any services to the National Grid Service. Nor

[12] www.ucl.ac.uk/research-computing/community

does UCL Research Computing assist UCL users in gaining access to NGS, other than by providing a page of information about applying for a UK e-Science Certificate and referring enquirers to the UCL Registration Authority. The co-ordinator estimated that there were fewer than twenty UCL users who need to use the scale of NGS, rather than UCL Research Computing facilities. (A)

UCL has four computational systems in the area of research computing. Three are clusters: Central Computing Cluster (C^3) which is 272 CPU, Linux based; Keter, a 224 core Sun cluster; and Altix, Linux-based SGI Altix 3700 with 56 processors (Itanium2 1.3Ghz/3 MB cache processors) and 112GB shared memory. These are all managed by the UCL Information Systems (IS) department. The other facility is the Condor high-throughput commodity computing pool, which utilises CPU power from the general UCL computer clusters, using the Condor resource management system. This is managed (historically) by UCL's Computer Science department in close association with IS, but will soon be handed over entirely to IS.

Access for UCL users to research computing facilities is currently managed manually by application forms and decentralised usernames and passwords.

9.2 Virtual organisations at UCL

There are collaborative research projects which require the use of shared research computing resources at UCL. In these cases, non-UCL researchers are approved for a username and password by a UCL "sponsor" and access is granted on a trust basis. However, the username and password is not associated on the system with a group of users - it simply provides access to the computing resources as a whole.

UCL contributes resources to the LCG (Large Hadron Collider Computing Grid), as part of London's contribution to Tier 2 of this grid. This resource comes from UCL's clusters via a pool of shared accounts on these clusters, which are assigned to applicants holding an e-Science certificate.

UCL has also found significant demand amongst research groups for using the VLE, Moodle, as a file-sharing tool (M).

Another example of a research community requiring identity management is the London Centre for Nanotechnology (U). This is a collaboration between UCL and Imperial College, giving rise to many academic collaborations between these two institutions and with others. The Centre also runs a startup offering bio-nano consultancy and processing to commercial clients, of whom some will require remote access to the Centre's facilities.

9.3 Future requirements

It seems that UCL is more likely to become involved in research computing collaborations outside the NGS than within it, based on mutual agreements such as one which is already likely with the University of Cambridge (A). Such agreements could be made on a case-by-case basis with bespoke terms and conditions, although there had apparently been a suggestion that the NGS could have a role as a broker.

UCL might possibly be more interested in participating in the NGS for research data storage rather than research computation.

UCL also has a desire to present all research computing facilities, including the NGS, through a single front-end for UCL users, to make them as easy as possible to access.

It is clear that federated access management (eg using Shibboleth) would have significant benefits for UCL's research computing, including:

- formal trust arrangements for external users of UCL research computing
- formal trust arrangements for ad hoc "grid" partnerships with other institutions
- single sign-on for UCL research computing with other UCL systems
- single access mechanism for local research computing and National Grid resources

10 Identity management in collaborative learning

UCL has been running some courses on its VLE, WebCT, for which either the students or the tutors are members of other institutions (M). These include a Dutch Translation Project[13], which is a collaboration between UCL, University of Cambridge and University of Sheffield. Experts and students from the three institutions collaborate in a translation project, using discussion forums. There is also a language learning course for schools, "CrossCall", run by UCL's CALT (Centre for the Advancement of Learning and Teaching). It is expected (M) that more collaborative learning will take place when UCL moves to Moodle as its VLE. This is because Moodle is open source and doesn't have the licence restrictions of WebCT.

At present, non-UCL users are given WebCT accounts, which stand alone from other credentials. It is intended that Moodle will be set up at UCL as a Shibboleth service provider, which opens up possibilities for federated access, where the non-UCL user belongs to an organisation with a Shibboleth identity provider and belongs to a federation with UCL. Other options for VLE login for non-UCL users include the use of UCL's Services System, where services are requested for the user on the basis of their connection with a UCL department. This would require appropriate "lightweight" computing accounts which may grant access only to the VLE.

Users only see courses which have been designated "public" or for which they have been explicitly enrolled, so access management is a separate process from account creation.

11 Identity management across HE and the NHS

UCL's Faculty of Biomedical Sciences has close links with NHS trusts including UCL Hospitals, Royal Free Hampstead and Whittington for the medical school, and others via the postgraduate institutes. In these cases, the libraries are joint ventures between UCL and the NHS.

In general, NHS employees who are also associated with UCL maintain two separate identities. They have separate sets of credentials for NHS and UCL computing resources, often three sets of credentials: for the NHS network, a departmental network, and the UCL central network. Access to UCL resources is not available for all employees of the NHS trusts with which UCL has a partnership. Only employees who are connected via teaching or research are eligible.

One key identity management issue between UCL and the NHS is the area of access to electronic library resources (O). Again, the set of credentials for accessing UCL resources is completely distinct from any NHS credentials, including NHS Athens.

The key to this access to UCL e-resources is the designation of UCL "Honorary Staff" status, which entitles the user to an Information Systems account with the appropriate access level (using authentication through a mix of Athens devolved authentication, EZProxy[14] and Shibboleth).

There may in future be a need for a further category/ies of affiliated staff, as library e-resource licences authorise any teacher of UCL students, not just those already qualifying for Honorary status, to access the resource.

[13] www.ucl.ac.uk/dutch/student_resources
[14] www.usefulutilities.com

UCL (including Library Services) is closely involved in the national NHS-HE Forum[15], which seeks to "co-ordinate and support network connectivity between the NHS and Universities involved with education and research in medicine, nursing and professions allied to medicine", including objectives to "promote electronic access of medical journals and content by students and clinical teachers" and "achieve two-way communication between NHS and HE networks, enabling secure anytime, anyplace, anywhere access by students and clinical teachers". Authentication is in scope of this forum.

12 Conclusions and Recommendations

The evidence of the audit is that UCL's identity management is quite coherent, and that central departments are aware of those areas in which improvements are still required. The UPI system works well as the centrepiece of the UCL identity, and must therefore be safeguarded, resourced and developed accordingly.

Access management (see section 4.3) is a major area which UCL is already committed to investigating. Areas for consideration include the requirements of the various systems and services in terms of authorisation rules, the mapping of attributes in order to define roles and user groups, and the mechanisms for assigning, modifying and revoking these roles.

Some themes for further work which arose from the audit are listed below, with the sections of the report to which they refer given in brackets.

Data ownership and workflows (4.2)
Person data is being gathered and stored in the primary systems and then re-purposed in secondary systems. In some cases, data which is required by secondary systems and is currently being entered into those systems could be gathered in the primary systems. This may require cultural change or incentives for primary data gatherers to source and supply data which are *only* required for secondary purposes. This is especially important in terms of any centralised access management strategy.

Use of federated access management (4.4, 5)
Beyond the current use of federated access management (FAM) for access to electronic library resources, it has potential for use in research computing, collaborative learning and research administration. This would require specification of attribute release policies, including user control over release of their personal data.

Identity management policies and responsibility
Throughout the audit, the distributed responsibility at UCL for identity management was apparent. It may be necessary to clarify centralised lines of responsibility for policy decisions, such as attribute definitions for institutional access management, and attribute release policies for FAM.

Lightweight computing accounts (5)
Needs were identified for an increasing range of non-standard or "lightweight" (no disk quota) computing accounts, for purposes such as VLE access, library e-resource access, and halls internet access for visitors. This could be managed in conjunction with the Services System for requesting such services, but would require cultural change in terms of the purpose of computing account creation and management.

Use of the identity card (3.2, 4.3)
The ubiquity of the new identity and access control card is leading to an extension of UCL's buildings access scheme. This may have implications for current workflows of assigning and maintaining access rights, as the volume of usage increases. It also increases the value of the card, as it becomes required for more purposes.

[15] www.nhs-he.org.uk

Synchronised sign-on (8.1)
The strategic drive towards synchronised sign-on has implications for the value of the central username and password, which need to be protected appropriately. Some users will be inclined to protect the credentials more carefully, but more is at stake if they do not. There are also questions around the scaleability of synchronised sign-on, such as which smaller systems should also be included in the scheme. The ongoing incorporation of departmental systems into this synchronisation is a major area of development.

Identity security and privacy (7)
In addition to the security and privacy aspects of areas already mentioned in this list, there may be scope for formal identity security policies, covering all aspects of attribute storage, transport and release, particularly as personal information is distributed across a wide range of systems and increasingly linked by a single identifier, the UPI. Authorisation policies for access to identity information could be audited separately, including the degree of self-service user control over personal information across the various systems.

The audit was only able to concentrate on central stakeholders in identity management, because of time constraints, so there remains ample scope for investigating the range of smaller-scale systems and practices, particularly within academic departments, and how these should interface with central practices, in order to build up a more complete map of identity management across the institution.

Appendix: Interview References

The following lettered references are used throughout the report when referring to topics raised in the interviews.

A Research Computing

B Financial Systems

C Human Resource Operations

D Access Systems

E Administrative Staff

F Records Office

G Student

H Registry

I Management Systems

J Information Systems

K Alumni Relations

L Academic Staff

M Learning Technology

N Library Services (Membership Services)

O Library Services (NHS links)

References from the following are also used, to refer to comments received during email correspondence with identity management practitioners.

P Research Administration

Q Departmental Administrator, Postgraduate Medical Institute

R Bloomsbury Theatre

S Departmental Administrator, Academic Department

T Facilities Administrator, Central Admin Department

U London Centre for Nanotechnology

V Departmental Administrator, Academic Department

W Administrative Desktop Service

X Systems Group, Information Systems