Good identity management helps academic institutions avoid financial loss, inefficiency in business processes and legal liability for mismanagement of personal data.

The JISC Identity Management Toolkit is designed to support ICT directors, managers and staff in universities and colleges.
# Table of Contents

**Toolkit Contents** .......................................................................................................................... 3
**About the Concise Printable Version of the Identity Toolkit** ............................................................ 4
**Terms of Use** .................................................................................................................................. 4
**Legal and Regulatory compliance** .................................................................................................. 4
**Navigating the concise printable Toolkit** ....................................................................................... 4
**Updates to the Toolkit** .................................................................................................................... 5
**Acknowledgements** ........................................................................................................................ 5
**Disclaimer** ...................................................................................................................................... 5

## 1 Introduction

1.1 What is identity ................................................................................................................................. 5
1.2 What is identity management (IdM) and why do we need to think about it? .................................. 5
1.3 IdM definition .................................................................................................................................. 6
1.4 Identity management in further & higher education (FHE) ........................................................... 7
1.5 What is the Identity Management Toolkit and why is it needed? .................................................. 8

**Toolkit Versions** ............................................................................................................................ 9
**Note** ................................................................................................................................................ 9

## 2 Identity Management Governance and Policies

2.1 Governance structure overview ........................................................................................................ 9
2.2 Provision of IdM services .................................................................................................................. 10
2.3 Consumption of IdM services ......................................................................................................... 11
  2.3.1 IdM system ................................................................................................................................ 11
2.4 Identity lifecycle and policy areas .................................................................................................. 11

## 3 Identity Management Systems, Components and Functions

3.1 Core IdM system components ........................................................................................................ 13
  3.1.1 Overview diagram .................................................................................................................... 14
3.2 Federated access .............................................................................................................................. 14

## 4 Defining Institutional Requirements:

4.1 Generating Specific Institutional Requirements .............................................................................. 15

## 5 Discovering and Auditing Current Institutional Identity Management

5.1.1 What is an Audit? ......................................................................................................................... 16
5.1.2 Why Hold an Audit? .................................................................................................................. 16
5.1.3 The Limitations of an Audit ....................................................................................................... 16
5.1.4 Customising a Smaller Scale Audit .......................................................................................... 16
5.1.5 Summary of Audit Process ........................................................................................................ 17

## 6 Gap Analysis

6.1 Establishing Actual Performance .................................................................................................... 17
6.2 Establishing Potential Performance ............................................................................................... 18
6.3 Common Gaps ................................................................................................................................ 18
6.4 Producing a Gap Analysis Report .................................................................................................. 19

## 7 An Institutional Roadmap for Identity Management

7.1 What is an IdM roadmap? ................................................................................................................ 20
7.2 Why is a roadmap useful? .............................................................................................................. 20
  7.2.1 Appropriate Pace of change ...................................................................................................... 20
7.3 Target System Types ...................................................................................................................... 20
7.4 Prioritising Targets ........................................................................................................................ 21
  7.4.1 Identifying initial targets ......................................................................................................... 21
7.5 Writing an IdM Roadmap ............................................................................................................... 21
  7.5.2 Roadmap Timetabling .............................................................................................................. 22
7.6 Conclusions .................................................................................................................................. 22

## 8 Ensuring Continuity of High Quality IdM

8.1 Politics and the Profile of Identity Management ............................................................................. 23
  8.1.1 What Happens When Identity Management is not on the Agenda ........................................ 23
  8.1.2 The Need for an Identity Management Strategy .................................................................... 23
  8.1.3 Formulating an Identity Management Strategy ...................................................................... 23
8.2 Applying Identity Management Principles to New Initiatives ...................................................... 24
8.3 User Communication ..................................................................................................................... 24

---

2 of 35
8.3.1 Introduction
8.3.2 User Education
8.3.3 Assessing the Impact of User Education
8.3.4 Self-service Identity Management

9 Designing and Managing an Identity Management Project
9.1 The Key Benefits of Good Quality Institutional Identity Management
9.1.1 Improved Security
9.1.2 Improved conformity with Legal Restraints
9.1.3 Improved Efficiency
9.2 Designing an IdM Project
9.3 Managing an IdM Project
9.4 Appointing Staff to Manage IdM
9.4.1 Information Security Manager/Officer
9.4.2 Identity Management System Manager

10 Selecting Supplier Solutions for Identity Management
10.1 IdM System Solutions
10.1.1 Capabilities of an IdM Solution
10.1.2 IdM Products
10.1.3 General IdM Software Considerations
10.1.4 Vendor Considerations
10.2 Tendering
10.3 Conclusions

Appendix: Identity Management Glossary

Toolkit Contents

1. Introduction to Identity Management
Start here! Defines basic terms and concepts of Identity Management used or assumed elsewhere. Should be read by anyone using the Toolkit.

2. Identity Management Governance and Policies
Describes the roles, structures and policies required for Identity Management and how they relate to Identity Management systems and processes. Useful for Chief Information Officers or Directors responsible for IT, and staff who need to draft or apply institutional policies.

3. Identity Management Systems, Components and Functions
The technical components and functions of Identity Management systems in an academic institution. Good background reading for IT service managers and staff, and anyone discussing Identity Management with potential system suppliers.

4. Defining Institutional Requirements
Functional requirements for each component of an Identity Management system, which may be useful in defining the objectives of an in-house implementation project or in detailed specifications to suppliers.

5. Discovering and Auditing Current Institutional Identity Management
A detailed guide to finding out the state of Identity Management in an institution with a comprehensive audit (based on work of the JISC Identity Project which developed and tested IdM audits in several universities).

6. Gap Analysis
Explains how to establish the current and desired states of affairs for Identity Management, gives a list of common gaps in FHE institutions, and suggests ways for developing a strategy.

7. An Institutional Roadmap for Identity Management
Producing an overall roadmap or programme plan. Prioritising major deliverables and milestones by achievability, cost and institutional impact.

8. Ensuring Continuity of High Quality IdM
Keeping a high profile for IdM in the institution, understanding how to apply IdM principles to new initiatives in
the institution, and ensuring that members of the institution know about the local and global aspects of IdM as they apply to their role within the institution.

9. Designing and Managing an Identity Management Project

Project management issues particular to implementing Identity Management, including key institutional benefits of improved Identity Management for use in an institutional business case.

10. Selecting Supplier Solutions

Where commercial procurement of systems or components is required, this section aims to help understand the IdM system solutions available, produce procurement criteria, and construct tender documents.

Identity Management Glossary

Not an exhaustive list but contains terms and abbreviations used in IdM, and in other sections of the Toolkit, and their meanings in an IdM context.

About the Concise Printable Version of the Identity Toolkit

Terms of Use

The Identity Management Toolkit is the copyright of JISC and the contributing authors. It is made available under a Creative Commons UK Attribution, Non-commercial, Share-Alike license. To discuss waivers or potential commercial use, please contact jiscinfonet@northumbria.ac.uk.

In plain English, the project to produce the Toolkit has been funded on behalf of the United Kingdom Further & Higher Education community (member colleges and universities of JISC) and all non-commercial users, including accredited universities and colleges worldwide, are encouraged to make use of material included in the Toolkit. If you wish to use or adapt text or graphics from the Toolkit in documents produced for use in your educational institution you may do so freely. Please credit “the JISC Identity Management Toolkit” and quote the URL “www.Identity-Project.org” in all derived material.

If you are intending to publish material derived from the Toolkit outside your own institution it should be covered by a comparable Creative Commons license; but we do not need you to ask us for a waiver if you intend to use such material only with staff and students of your own academic institution. We would be very pleased to hear, though (please email jiscinfonet@northumbria.ac.uk) about any use of material in the Toolkit.

Cover graphics used in printed/printable versions of the Toolkit are copyright HEFCE on behalf of JISC and used under a Creative Commons UK Non-commercial, Attribution, Non-derivative licence; which means that these should not be re-used in material other than the Toolkit without permission from JISC.

Legal and Regulatory compliance

Information about legal and regulatory requirements in all sections of the Toolkit is considered accurate by the authors at the time of writing (August 2009 to February 2010), and have been checked again on revision (February to August 2012). To ensure compliance with current rules and legislation, up to date independent and qualified advice should be sought to inform any decisions by your organisation.

Navigating the concise printable Toolkit

The concise printable toolkit contains a subset of the text of the complete printable Toolkit, which is as far as possible identical to the contents on the online Toolkit. The Contents and Summary briefly outlines the purpose and intended readership of each main section and the entire content is indexed by page number at the start of the document. As far as possible references by URL to external documents and resources in a section are repeated under the heading “Resources” at the end of the document, with the URL in human-readable form. Some cross-references to internal resources (contained in the online version of the Toolkit) will be to the online section to which an item is attached. The Toolkit also contains a Glossary of terms used, as an appendix.
Updates to the Toolkit

After initial publication (August 2012) of the Toolkit updates and corrections may be made to the online version of the Toolkit. Unfortunately, there is no facility for incorporating such changes into the PDF versions of the Toolkit.

Acknowledgements

See https://identitymanagementinfokit.pbworks.com/w/page/51837099/ToolkitCredits_Version2 for a list of participants in the compilation of the Toolkit.

Disclaimer

The information contained in all published versions of the Identity Management Toolkit (the Toolkit) is for general information purposes only. The information is provided by JISC and the partner institutions involved in the project (the Project) and while we endeavour to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the Toolkit or the information, products, services, or related graphics contained in the Toolkit for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of the Toolkit.

Through links provided in online and printable versions of the Toolkit you are able to access other websites which are not under the control of the Project. We have no control over the nature, content and availability of those sites. The inclusion of any links does not necessarily imply a recommendation or endorse the views expressed within them.

Every effort is made to keep all versions of the Toolkit available and functional. However, the Project takes no responsibility for, and will not be liable for, any version of the Toolkit being temporarily unavailable due to technical issues beyond our control.

1 Introduction

1.1 What is identity

One definition of identity (Oxford English Dictionary) is:

The sameness of a person or thing at all times or in all circumstances; the condition or fact that a person or thing is itself and not something else.

We are given a name at (or shortly after) birth. Within a small community a name may be sufficient to refer to a specific person unambiguously. However, beyond that community, a name will often not be unique, or there may be no means to verify that someone is who they say they are. Knowing that someone is who they say they are is the first basis of trust, entitlement and accountability.

All modern societies have found it necessary to provide means by which identities may be independently verified, e.g. birth certificates and passports, and proof of identity is a pre-requisite for many activities, e.g. opening a bank account.

The above definition should not be taken to mean that identities do not change. In fact, over time, many attributes relating to an identity will change e.g. when someone adopts the surname of their spouse, and coping with such changes is one of the challenges of identity management.

1.2 What is identity management (IdM) and why do we need to think about it?

Identity management, in a general sense, includes all the processes and systems that allow the creation, retrieval, update, verification and destruction of identities and information relating to identities including any
rights / authority granted to the identities. It is important to note that identities have been, and continue to be, managed using paper-based systems operated by people. In addition, many IT based identity management systems are used to create artefacts (e.g. identity cards) which may be subject to visual checks and/or machine-based verification.

Identity management in computing involves the mapping of real world identities to electronic identities and ensures appropriate use of IT systems. It is important because the use of IT systems has become pervasive in many aspects of life. IT systems may be, and are, misused to breach confidentiality, perpetrate fraud and disrupt critical activities. Furthermore, legislation has been introduced that place legal requirements on businesses to protect personal privacy and to ensure the confidentiality and security of their information. Holders of personal data must not only be registered under the Data Protection Act, but also take adequate steps to protect that data from unauthorised access.

Aside from security concerns, consistent and accurate use of identities across IT systems increases organisational efficiency and flexibility, and improves user experience, leading to reduced costs and competitive advantage.

1.3 IdM definition

Wikipedia defines identity management as:

In information systems, identity management is the management of the identity life cycle of entities (subjects or objects). An identity management system:

1. Establishes the identity
   1. Links a name (or number) with the subject or object;
   2. Re-establishes the identity (i.e. links a new or additional name, or number, with the subject or object);

2. Describes the identity:
   1. Optionally assigns one or more attributes applicable to the particular subject or object to the identity;
   2. Re-describes the identity (i.e. changes one or more attributes applicable to the particular subject or object);

3. Follows identity activity:
   1. Record and/or provide access to logs of identity activity
   2. Optionally auto-analyze behaviour patterns of the identity

4. Destroys the identity

In practice, IdM is concerned with:

- managing identity information
- integration
- security and access control
- compliance and governance

Naturally organisations have a sense of ownership over identities they manage and are most concerned with their own activities and responsibilities, however, from the perspective of an individual this is not always a satisfactory approach. An individual often has affiliations with other organisations leading to multiple identities across a range of systems. There are a number of initiatives aimed at giving individuals more control over their identity and this is an area where FHE organisations need to be engaged in order to meet user expectations and to facilitate collaboration.

All organisations operate systems which would fall under the definition above, however, in general, most organisations have sub-optimal and ad hoc systems which have evolved rather than been designed or planned. In this document an identity management system (IdM system) refers to a system which:

1. is secure and allows appropriate restrictions on the use of IT systems and other facilities
2. complies with legislation
3. has been designed and sized to manage all identities relevant to an organisation, including external identities
4. supports organisational processes in an integrated, timely, flexible and efficient manner

or, in summary, is fit-for-purpose.
1.4 Identity management in further & higher education (FHE)

FHE organisations have the same security and legal obligations as other organisations. As in any sector FHE organisations also have many similarities:

- large intakes of new identities at least once per year
- a strong ethos of openness and collaboration with academics and students collaborating on projects and visiting partner organisations
- partnerships within HE and with businesses and the local community
- medical schools have close links with the NHS
- continuing relationship with alumni
- IT systems developed for and/or targeted at the sector e.g. Student record systems, virtual learning environments (VLEs) and Library systems

There are benefits to the sector in adopting common standards-based approaches:

- organisations may choose systems from different vendors without being locked in
- the sector can influence the development of standards
- organisations can share relevant experiences
- funding organisations are more likely to contribute to infrastructure if it will be used throughout the sector.

The complexity of FHE organisations is summarised in the diagram overleaf.

Key challenges include:

- the number of individuals involved in the organisation i.e. thousands to tens of thousands
- managing the many different membership types
- providing a wide range of systems and facilities to support the wide range of activities undertaken
- controlling, as appropriate, access to systems and facilities
- maintaining reliable, accurate and timely data across systems
- overlapping responsibilities and systems e.g. students may be associated with a course, department, school and faculty which may operate local systems
- allowing external users access to systems and facilities
- allowing users to access external systems and facilities
- providing a coherent user experience, particularly when users may have more than one role i.e. a member of staff may also be an alumnus enrolled on a masters course whilst applying to do a PhD on completion of their current studies.
- different membership types are generally the responsibility of different departments and are managed in different systems
- access to systems is often managed, by different teams, in system-specific ways
- data captured to support one activity or system is not available to othr systems or is inadequate for use in another system

IdM can help meet these challenges, and, in so doing, support the core activities of FHE organisations by providing a coherent model of the organisation and its members, activities, facilities and systems, which can be managed in an efficient and consistent way.
1.5 What is the Identity Management Toolkit and why is it needed?

The Toolkit is intended to support high quality Identity Management in the FHE sector, focussing on the specific challenges which are to be met in the sector. The JISC Identity Project found that there was little consensus, even within organisations, on what IdM is, along with a number of common gaps in IdM practice. The Toolkit aims to help institutions address these problems.
The material in the Toolkit is intended to contain material applicable to as wide a range of organisations from the FHE sector as possible. This means that it is important to decide which material is relevant to your particular institution or organisation before making use of it. The intention is also to be advisory rather than prescriptive, and the Toolkit should be read in this light: the material should be adapted to fit the local requirements and culture, not necessarily used precisely as it appears here. The Toolkit should be applied in a way which is tailored to the organisation’s size and complexity, recognising the environment within which it operates. It is also important to base any substantive work on an understanding of the whole Toolkit, not just the concise version.

**Toolkit Versions**

The Identity Management Toolkit exists in five versions, as revised in 2012, all available for download or browsing from www.Identity-Project.org. These are:

- **The online Toolkit, version 2.** This version consists of web pages and includes downloadable resources, such as source files to enable diagrams to be re-used and adapted. While the main content of this will remain essentially static, there is also an associated blog which will be used to post additional material from time to time.
- **The complete printable Toolkit, version 2.** This is a PDF document consisting of the full textual contents of the online Toolkit, without the associated downloadable resources.
- **The concise printable Toolkit, version 2.** This is a more accessible PDF document, intended as an introduction to the complete Toolkit, and includes some content and summaries of the remainder.
- **The older online Toolkit, version 1.** This is still accessible, but is now replaced by version 2.
- **The printable version of the older online Toolkit, derived from the online content, also available as a PDF from www.Identity-Project.org.**

This document is the concise printable Toolkit, version 2.

**Note**

Throughout the Toolkit, the abbreviation FHE is used for “the further and higher education and skills sector”, and FHEI for “FHE institution”.

**2 Identity Management Governance and Policies**

**2.1 Governance structure overview**

The diagram overleaf outlines the general roles and relationships required to operate an effective IdM system. How these are mapped onto actual jobs and individuals/groups will of course vary with the differences in size, traditions and existing structures of FHE institutions, and some roles may be combined.

Elements of the diagram are discussed in the following sections, however, it is worth emphasising the need for continuous awareness of other initiatives within the institution. In recent years uncertainty about FHE funding, larger student loans and new regulatory requirements have prompted many FHEIs to embark on significant organisational change to both support and academic services, in order to increase efficiency and to allow greater focus on student experience. The scale and nature of the changes has made many organisations review and enhance their existing programme/project management infrastructure/methodologies including looking at new frameworks and tools e.g. enterprise architecture and service oriented architecture.

It is important that the IdM project team and sponsors are aware of ongoing change in the institution and pro-actively engage with other projects to raise awareness of what IdM is and ensure that IdM is taken into account. For example, projects which involve new systems and/or business process improvement, including formalising roles and restructuring departments will also have requirements around access and privilege management which could benefit from workflow available in an IdM system. While each institution will have its own process for managing and co-ordinating change, it is recommended that consideration of IdM be made a formal part of any change process.
2.2 Provision of IdM services

For identity management to be effective it must have support from the highest levels of the organisation as well as the main stakeholders. A representative high level board with decision making powers should oversee all aspects of IdM practice and be accountable for that practice across the organisation, ensuring consistent and effective practice. Most board members will not be IdM experts but will be able to draw on expert knowledge. The board should meet on a regular basis. All requests, decisions and policies should be transparent and documented. The board should ensure that policies are reviewed on a regular basis and that IdM practice is audited to ensure compliance with the law and the wider goals of the organisation. For FHE institutions that have an individual in the role of Chief Information Officer (CIO), it will be appropriate for the CIO either to assume the role of Chair of the board, or to be the senior staff member reporting to it.

IdM operations should be headed by a senior member of staff with relevant IdM experience. The IdM director would be responsible for day to day operations and would report to the IdM governance board. The director would be expected to keep abreast of identity management risks and issues, and, in particular, their potential impact on the organisation and the higher education sector in general. In smaller FHE institutions this may be the CIO; in larger ones this role may report to the CIO.
Implementation of an IdM system will require integration with many systems and involve many systems teams. It is important that detailed technical options are agreed and subject to appropriate scrutiny by, for example, an ICT board, which has responsibility for overseeing technical infrastructure.

Technical staff will be required to maintain and support the IdM system and users of the system. Staff in this department will have an important role in spreading IdM competence and ensuring compliance. They should have clear guidance on how and when to escalate issues to the IdM director, who, in turn, can resolve issues or escalate issues to the IdM governance board.

Most organisations will already have structures and policies to deal with data protection and security issues. With the development of an IdM system it is important to clearly set out roles and responsibilities and to ensure that experts in the different areas work together and are able to obtain appropriate legal advice, particularly when legislation changes, new legislation is introduced or legal precedents are set.

Internal and external auditing services should be available which are independent of those operating the IdM system.

Due to the impact of IdM on all areas of the organisation it would be desirable to have representation on other governance bodies for the institution, and perhaps for those bodies to nominate members of an IdM governance board. The names, structures and memberships of such bodies varies widely across FHE institutions and so the Toolkit will not suggest examples.

### 2.3 Consumption of IdM services

Ultimately the perceived success or otherwise of an IdM system will largely be judged by those who have to use it directly or interact with systems which depend on it. The actual success also depends on how effectively people use the system which, in turn, will depend on appropriate configuration, effective training and support, awareness of responsibilities, and the management and cultural factors which lead to responsibilities being taken seriously and acted on at all times.

#### 2.3.1 IdM system

All data held within the IdM system should be classified for privacy/security reasons and the purposes for which data was collected, and may therefore be used, clearly documented. More detailed policy is required for confidential data to set out who exactly is able to view (and create, modify or delete) data.

A primary function of an IdM system is to ensure that such a classification is adhered to internally and externally by systems which receive controlled data. An important part of projects which lead to the collection of new data and/or the integration of new systems is to ensure that data classification analysis is carried out, communicated, and that a risk assessment is carried out along with implementation of any measures which will mitigate any risks.

The IdM system itself will provide identity information to many other systems often operated by staff in other organisational units. As each system is integrated there should be a formal review of what data is transferred between systems and why. Each integration should be documented and any changes subject to review.

### 2.4 Identity lifecycle and policy areas

The diagram overleaf shows the identity lifecycle and is used to help group policy areas.

#### (a) Application / invitation

HE and FE organisations process many applications, from staff and students, each year, leading to the collection of identity-related information in both electronic and paper form. In addition, HE and FE organisations may invite individuals to participate in a variety of collaborative activities, such as research, which require those individuals to access facilities and services.

Applications may be tracked in one or more systems and these systems may form part of the IdM system, allowing, for example, applicants to track the progress of their application.

#### (b) Unsuccessful application

Many applications will, ultimately, be unsuccessful, and the records involved need to be appropriately handled.
Following a successful application, or acceptance of an invitation, an individual normally enters into some contractual arrangement with the organisation. The organisation will then create a new identity, and provide some form of credentials which the individual uses to access facilities and services. Individuals may be linked to a unique (preferably opaque) identifier that has not previously been used. Re-use of personal identifiers may, inadvertently, allow the new identity to access some of the facilities and services to which the old identity was entitled.

---

1. Linked to a unique (preferably opaque) identifier that has not previously been used. Re-use of personal identifiers may, inadvertently, allow the new identity to access some of the facilities and services to which the old identity was entitled.
assigned a membership type\(^2\) and their roles and affiliations recorded.

**(d) Role / status changes**

Many individuals are members of the organisation over a number of years during which time they may be promoted, change role, move to a different department have temporary leave of absences etc. Each change may be reflected in changes to relationships and affiliations with subsequent changes in entitlement to access facilities and services.

The organisation should take active measures to ensure that members are aware of their general responsibilities with respect to IdM. Particular roles may require specific training.

**(e) Integration**

An IdM system is designed to be an authoritative central hub of identity information. External services may access information through APIs or directory services, or data may be provisioned to the external service. It is crucial to ensure that information security is maintained when data is in transport and when stored in a new location. Changes in the IdM system should be propagated to external systems in a timely manner. The ease and speed of propagating changes may be a factor when procuring systems which need to be integrated with the IdM system.

**(f) Leaving the organisation**

In many cases it is predictable when an individual will leave the organisation, or there is reasonable notice e.g. retirement, end of contract, end of studies, resignation and redundancy. Individuals should be reminded, in good time, to retain any personal information held in the organisation's data stores and ensure that business information is moved to appropriate data stores where colleagues have access.

Once an individual leaves the organisation they should be removed from external systems. An individual may return to the organisation and be assigned their old identifier, but they should not necessarily have access to the same facilities and services as before.

In cases of suspension, dismissal, failure to complete studies or due to disciplinary sanctions there may be a need to remove some, or all, access to facilities and services quickly.

### 3 Identity Management Systems, Components and Functions

This section explains the technical components and functions, in general terms, of Identity Management required by an academic institution. It would form suitable background reading for IT service managers and staff who will be responsible for commissioning, implementing or maintaining IdM systems and data.

#### 3.1 Core IdM system components

The components listed here correspond to distinct logical functions of an IdM system, rather than the way software components are designed and bundled together. Descriptions of the features are available in the full printable Toolkit or the online version.

*Identity repository and lifecycle management:* Common features include User categories; User records; Credential management; Self-service; Workflow; Organisation modelling; Provisioning/synchronisation; Auditing and reporting.

*Authentication service:* Common features include Credential validation; Level of Assurance (LoA); Single sign on (SSO); Proxy authentication; Federated access.

*Authorisation service:* Common features include Rules; Policy; Roles; Groups; Delegation; Proxy; Provisioning; Auditing and reporting.

*Directory service:* Common features include Identity discovery; Lightweight Directory Access Protocol (LDAP); Schemas; Virtual directory.

*Groups service:* Common features include Dynamic groups; System maintained groups; Ad hoc groups; Personal groups; Inheritance; Name space; Self-service; Membership expiry; Attributes; Authorisation; Provisioning; Auditing and reporting

---

2 Should cover grey areas such as applicants, new recruits who have not officially started, recent leavers, alumni, people on maternity leave or sabbaticals and students who have finished one course but expect to start a new course e.g. undergraduate -> postgraduate, and atypical users.
3.1.1 Overview diagram

In principle, the components introduced above may be loosely coupled and/or may be provided by different vendors/open-source projects. The diagram below depicts this, showing a logical separation of functions.

3.2 Federated access

The diagram below and the following sections provide an overview of how identities from one organisation may use Shibboleth to gain federated access to services hosted by another organisation. Membership of a federation places obligations on members which allow members to trust identity assertions provided by other members.

An organisation may also choose to use this model internally. The advantage of this approach is that it provides a single, consistent means of authenticating users and implementing access control.

The Shibboleth-based UK Access Management Federation for Education and Research is supported by JISC, with some support for the schools sector from JANET(UK). The federation website gives a list of benefits for joining the federation³.

4 Defining Institutional Requirements:

This section outlines the general technical requirements an institution should specify for the implementation

³ [http://www.ukfederation.org.uk/content/Documents/Benefits](http://www.ukfederation.org.uk/content/Documents/Benefits)
of IdM. These cover the key areas for any IT system such as usability, availability, integration, security and sustainability. For each key component of an IdM system (credential management, single sign on, provisioning/synchronisation, workflow and authentication/authorisation) specific requirements are listed. It is recommended that the specific requirements be collated as part of the audit process, as they will vary from one institution to another depending on existing IdM practices and systems. The language used in this chapter implies a packaged solution, however, an IdM system may be composed of components from different suppliers and include systems developed in house. Whatever the solution significant local customisation and integration will be required.

4.1 Generating Specific Institutional Requirements

In order to progress with work on Identity Management, it will be necessary to go from general requirements to ones which are specific to the institution wishing to carry out the work. This is essentially done by understanding the current situation regarding IdM, then deciding what needs to be changed and how best to carry out this change.

One important method to find out the current state of affairs is to carry out a comprehensive audit (or to customise a cut-down version of the audit to fit local requirements). Smaller scale exercises, such as discussions among stakeholders involved in the provision of the major IdM functions of the institution, or the use of surveys about satisfaction with the IT Services department's work. More information is given in the Gap Analysis section, which also discusses how to use this material to create an analysis of the work which needs to be done.

Business analysis and requirements analysis tools such as the development of user stories relating to IdM (from individuals such as developers seeking to integrate their work with central IdM, or IdM stakeholders in general), as used in agile development, and process modelling can be used. The assistance of a trained business analyst may well prove useful in this task. The lists of general and functional requirements appearing earlier in this section are likely to provide at least some requirements which are relevant to the specific situation being addressed by the work.

Whilst it is likely that those involved will have considerable experience in the development of requirements, it is worth bearing mind that they should:

• contain sufficient details that they can be implemented
• include measurable tests to check that they have been met by the implementation process
• include non-technical requirements as well as technical ones
• ensure that relevant procedures and documentation are produced
• ensure that security and privacy concerns are properly addressed

See also how to manage an IdM project below.

5 Discovering and Auditing Current Institutional Identity Management

This section details an important method which can be used to find the state of IdM in an institution: a comprehensive audit. This is a large scale method which endeavours to find all the important business processes within the institution which relate to the management of identity. It should cover the whole identity cycle from user registration to expiry, and its scope is wide enough to include small scale unofficial IdM, and non-IT based IdM, such as paper based access control lists for access to specific physical resources.

For FHE staff who might want to propose, organise, and carry out an audit, this section details:

• what is meant by an audit
• how to propose an audit to senior management
• how to project manage an audit
• how to find those who carry out IdM in an institution
• how to find out how IdM is carried out by these people
The key results of the audit should feed into a gap analysis and the most important benefit is obtained through the use of the gap analysis to improve security and productivity in an institution through improvements in IdM processes.

The concise version of the Toolkit only includes the introduction to this section compared with the complete versions, which should be consulted for details of the operation of an audit.

5.1.1 What is an Audit?

A audit is a comprehensive, detailed study of an organisation's identity management systems. The aim is to find out how procedures relating to identity management are carried out, even if some of the practitioners do not realise they are identity managers.

The audit process described in this section describes a large scale project to discover as much as possible of an institution's IdM processes. This may not be considered an appropriate use of resources, though the more that is known, the easier it is to find problems and plan to fix them. Smaller organisations, in particular, will not necessarily have to carry out such an elaborate process to obtain much useful information; the processes and requirements for IdM are likely to be simpler, and the resources less likely to be available. Thus, the material in this section is intended to be viewed as advisory rather than prescriptive, and should be freely adapted to local circumstances.

5.1.2 Why Hold an Audit?

A more detailed business case for holding an identity audit is contained in the material in the complete Toolkit versions. However, the essential reason for carrying out this process is that FHEIs are complex organisations, with many people likely to be carrying out identity management tasks (sometimes without actually realising that they do so), and where there are often processes which are poorly documented, designed by tradition rather than with considerations such as security in mind, or duplicated between departments and/or individuals. As technologies such as Federated Access which rely on accurate identity-related information being available become commonly used, it is important to ensure that identity management processes are streamlined, documented, secure and accurate. Many of today's business decisions (particularly relating to IT procurement) involve identity management as potential requirements or affected by the outcome, and a detailed understanding of existing identity management processes as provided by an audit will provide the necessary input for the decision making process.

5.1.3 The Limitations of an Audit

- An audit is not a survey. It is not designed to obtain quantitative results with measurable standard deviation as an opinion poll. The sample questioned in an audit is small, and carefully hand picked.

- The accuracy of some of the opinions obtained from interviewees is limited. Because of the nature of the sample, the answers to some questions will be coloured by greater knowledge of the identity management environment of the institution than a survey. (This is likely to lead, for example, to higher measures of satisfaction with the way that the institution manages personal data.)

- An audit does not measure actual behaviour, but interviewee's reports of their behaviour. This may make them less likely to admit to flaws in the processes and in how documented processes are carried out.

Other activities can be carried out in parallel with an audit to provide supplementary information of the sort that is listed here.

5.1.4 Customising a Smaller Scale Audit

There are two main reasons why an institution might want to consider cutting down the full audit process described in this section. There may not be sufficient resource to spend the time and effort which the full process requires, or the organisation might be of a nature where the full process is not appropriate - IdM processes in a smaller institution will be simpler, and some organisations may not carry out some of the
functions being investigated (see for example the UK Data Archive’s case study, which applied an audit of this type in a body which acts principally as a service provider).

There are two ways in which an audit could be cut down in scope. The first is simply to talk to fewer people, concentrating on the people involved in the core IdM processes. This runs the risk of missing important information, as issues to address are less likely to occur in these large scale, relatively well understood and centralised services dealing with the main categories of user than where people have invented their own procedures for ad hoc IdM, or where the individuals whose identity is being managed are unusual. However, there would be considerable time savings in the discovery phase of the Audit, as most of the individuals involved will be well known and probably key people within departments such as SIS or Computer Services. Interviewing fewer people will also make the investigation stage easier and there will be less material to interpret for the analysis stage. Effectively, this approach would make the Audit a series of meetings with a representative group of stakeholders. Such an approach requires considerable knowledge of the existing state of official IdM practices at the institution.

The second way to cut down an audit would be to concentrate on a specific gap which is likely to occur. (The Gap Analysis section includes a discussion of the major gaps which commonly occur in FHE Identity Management.) Again, it will be relatively simple to track down individuals involved in relevant processes, and there will be less information to gather and analyse. The risk here is that the overall picture will be lost as IdM is investigated from one particular angle.

5.1.5 Summary of Audit Process

We start by giving a broad outline, to put the details discussed in the following four sections into context. The work required for an audit divides naturally into four phases, first preparation, then successively IdM discovery, investigation and analysis. It is important to realise that all the details are intended as guidance rather than to be as strict rules, to allow for adaptation to the culture of the institution carrying out the audit. In many cases, more suggestions will be given than are practical, so choices will need to be made.

The preparation phase consists of finding an appropriate individual to take on the role we have designated “key researcher” (abbreviated KR), and ensuring that they have the knowledge required to carry out the audit (such as sufficient technical understanding to engage experts in the configuration and use of complex software). The KR will need to plan the process, looking at the various options suggested here and adapting this process to the local institutional culture, as well as establishing a timetable for the audit. Overview of the process (by an appropriate group, e.g. an IT Manager’s Forum, and backed up by a senior member of the institution) is also set up in this phase.

The IdM discovery phase aims to find as many individuals as possible within the institution who may carry out duties which amount to identity management. From these identified individuals, a target list of those to be interviewed needs to be selected, and then interviews scheduled. A parallel process of documentation discovery should be carried out at the same time.

The IdM investigation phase contains the interviews themselves, and the basic writing up of the information gathered this way. This guide discusses several methods for carrying out this process, with the key aim of making the next phase as easy as possible.

The final phase, the IdM analysis phase, aims to produce a coherent report out of the materials that have been gathered, with a description of the institution’s current identity management regime and recommendations for consideration by senior management.

6 Gap Analysis

A gap analysis consists of three parts: an understanding of the current state of affairs, an understanding of the desired state of affairs, and the development of a method to get from the first to the second. For IdM at an FHE institution, all three will depend to a significant extent on local conditions, which cannot be developed here. In this section, we look at means to establish the current and desired states of affairs for IdM, give a list of common gaps (derived from the work carried out by the Identity Project), and make some suggestions as to how a strategy can be developed.

6.1 Establishing Actual Performance

Potential sources for doing this include the following:
• The Report from an IdM Audit

• Password experiment. This is a method to measure the state of knowledge about security and privacy among end users.

• Use of existing surveys. Many institutions carry out periodic (frequently annual) surveys of user satisfaction with IT Services departments. Questions relating to IdM practices can be inserted into such a survey.

• Analysis of help desk enquiries where these relate to IdM. Where help desk software is used which allows categorisation of the type of a query, this becomes a comparatively simple task - and provides useful measures of a reasonable degree of accuracy which can be gathered over a lengthy period of time.

• Keeping records of a variety of IdM related metrics over a period of time. This would be particularly useful for measuring the effectiveness that work on IdM has in improving the situation. Naturally, the metrics to be used (and how they’re measured) would depend on the nature of the gap involved, and the figures will not necessarily indicate the presence or absence of a gap (as there are no benchmarks to measure them against).

6.2 Establishing Potential Performance

In the UK FHEI context, the minimal potential performance should be based on:

• legal and regulatory requirements. Some information about these is given in the introductory section of this Toolkit, but the institution’s Data Protection Officer will be able to describe the details of how they apply and should know how IdM systems relate to them.

• contractual requirements necessary to carry out the normal activities of a UK FHEI (e.g. adherence to stipulations in electronic resource licenses purchased by the library - though these are not always written with IdM security in mind and it may be the case that it would be preferable to renegotiate some than comply to the letter)

• the requirements (and recommendations) for UK Federation membership. It should also be remembered that decisions made by an institution as an Identity Provider will affect the way that institutional members are described to Service Providers, and thus the design of any IdM work needs to ensure that it will not affect the access of members to external resources. In the Federated Access Model, a Service Provider is dependent on the quality of the IdM processes of the Identity Providers used to access its resources.

The systems, components and functions section of the Toolkit, describing the components of an ideal system, is likely to help identify technical gaps. This description will need to be analysed to see which components give appropriate requirements for the IdM of the specific institution. Generic requirements are gathered together in Section 4, Defining Institutional Requirements, and these can also be used as a basis for establishing potential performance.

Many institutions will already have ideas about where gaps exist, and these will often be directly pointed out by interviewees in an IdM audit. However, it is difficult to produce a gap analysis without a clear idea of the potential performance requirements, and for this purposes an institutional IdM strategy is an invaluable aid. Some suggestions which may aid the formulation of an IdM strategy can be found in the Toolkit section on governance. (Of course, the lack of an overall strategy may be one of the gaps that needs to be addressed.)

6.3 Common Gaps

The JISC funded Identity Project carried out a number of audits following the model described in this Toolkit in UK FHEIs during 2007 in conjunction with a survey sent to all UK FHEIs. It is clear from these audits and the survey that institutions are likely to find gaps, and that some are common to many institutions. The project’s report Common Problems/Solutions, Best Practice, Future Developments (no longer available) collected these issues together; a summary is given here.

One topic which has achieved prominence since the conclusion of the Identity Project is the relationship

4 http://theidentitytoolkit.wordpress.com/2012/08/02/measuring-user-security-behaviour/
5 http://www.ukfederation.org.uk/content/Documents/FedDocs
between institutional IdM and external systems utilised by many of the institution’s users but not controlled by
the institution, such as Facebook, OpenID and other social media sites and technologies, especially as it
starts to become possible to embed institutional services in them (such as Facebook applications listing
library books the user has out) or use them for access to other systems which may seem more official (such
as Google Docs stores of documents produced by academics available to students, or twitter hash tags for
discussion of courses).

Clearly, there may be other gaps which are specific to a particular institution, and these should also be
considered. Tools such as the audit should uncover these gaps almost as readily as those which occur in
many FHEIs. It is also likely that the different local situations make it sensible to subdivide some of these
gaps, or that there will be specific local issues which need to be listed.

- Lack of Commonality of Definition of “Identity Management”
- Formal Procedures
- Heterogeneity - Independent, Disparate Systems
- Common Standards and Central IdM Administration
- Limited Deprovisioning
- Identity Management Data Quality
- Use of Non-unique User Credentials (simultaneously per individual)
- Re-use of Identifiers

6.4 Producing a Gap Analysis Report

For each identified gap in performance, the report should include as much as possible of the following
information:

1. Description of the current performance (Baseline)
2. Description of change(s) suggested: Changes should have a measurable effect
3. Description of the desired performance (Target)
4. Reason for change (Rationale)
5. Degree of change (i.e. estimates for how difficult will it be to achieve the change, and how beneficial
   will it be to do so, and whether the gap will be completely filled - which may not be possible in some
cases)
6. How to measure that the change is successful

This listing is effectively a template for the gap analysis, and is based on the Goal Gap Analysis found at the
Office of Research and Institutional Effectiveness, Butler Community College (no longer available). Ideally,
the change should be as objectively measurable as possible, though defining a usable measure may be hard
to do and may require work beyond that already carried out.

It is also useful to provide a summary analysis of the gaps for visualisation, and one method of doing so is to
give scores for each gap for:

- Fitness: how good is the current practice
- Target: what can reasonably be achieved (measured against perfect performance)

Each of these will differ widely between institutions (and of course the scores given will be arbitrary estimates
from the authors of the gap report), but should provide a useful way to present the gap information to senior
management.

A gap analysis report should also include overall prioritisation of the work to be done; ideas on which gaps
could be tackled together; and ideas for including gap filling in other initiatives or work which needs to be
done as a matter of course (e.g. with planned upgrades to an existing IT system).
7 An Institutional Roadmap for Identity Management

This section deals with the production of an overall roadmap or programme plan for the actions an institution needs to take in order to improve identity management. It discusses the prioritising of major deliverables and milestones identified by an audit and gap analysis by factors of achievability, cost and institutional impact.

7.1 What is an IdM roadmap?

A roadmap is essentially a document that describes firstly how the future state of IdM should function, and secondly describes a prioritised plan of work that will get IdM to that state. This can be used to split up an IdM implementation strategy into various phases. It should use as input an assessment of the current state of IdM as would be uncovered during an IdM audit and a gap analysis produced from this assessment, along with a description of the required changes needed to fill the identified gaps.

An IdM roadmap should include an implementation timeline with major milestones and key deliverables identified. Other things that need including in a roadmap are an identification of risks and mitigations against those risks and methods for monitoring and measuring progress against the roadmap.

7.2 Why is a roadmap useful?

In many cases, the amount of work necessary to implement and embed a central IdM system within an academic institution is likely to be large and complex. A “big bang” approach to this process - whereby all components are installed and configured in essentially one go - will in almost all cases not be appropriate, as the sheer amount of work and integration necessary will be overwhelming to implementers and users.

Thus, the more sensible approach is a measured, phased approach to implementation with an appropriate pace of change. Constructing a roadmap to prioritise the overall plan of work into such a measured, phased approach will maximise the likelihood of success of an IdM project. This road will identify an order of work that will gradually encompass all of the systems that are ultimately required to be integrated within the overall solution.

7.2.1 Appropriate Pace of change

The experience of those who have already gone through the process of implementing and integrating IdM systems consistently shows that new systems should be connected gradually to an IdM solution.

One of the main reasons for this is that any legacy system - where “legacy” here means any application with any existing data in it - will have its own quirks and intricacies in operation and data that it cannot be hoped to understand in full without the aid of time. Even a full understanding of data within a system at a particular point in time is often not enough - it can take at least one academic cycle (i.e. one year) to understand how that data changes over time. For example, data that is updated in a timely manner during academic term time may be much slower to be updated over the summer break; data that is generally kept up to date throughout the year may suffer timeliness issues at the start of the academic year due to sheer volume of change at this busy time of year; and other such issues causing data quality and timeliness to vary over time.

Ensuring that the pace of change is appropriate to an academic institution, and not needlessly rushing the process, will mean that time can be taken to really understand each component in an IdM system; this knowledge will increase the chances that the IdM implementation will be deemed a success.

7.3 Target System Types

IT systems connected within an IdM implementation can be split conceptually into two main types, Data Authorities and Data Consumers.

Data Authorities are mainly sources of identity data. Within an academic institution, these will usually include the Student Records System (SRS) – the data authority for student identity information – and the HR system – the data authority for staff identity information. Further sources of identity data may include things such as Alumni systems, NHS systems, etc. Also, there will often be systems for manually managing identity data of non-standard users who do not exist within any of the "standard" data authorities.

Data Consumers, on the other hand, are mainly users of identity data. Within an academic institution, these
will include things such as network account provisioning/de-provisioning mechanisms, email account management systems, VLEs, institutional identity card systems, physical access systems, etc.

Note that many systems may technically be both a source of, and consumer of, identity information. For example, a SRS may be the authoritative data source for student identity information such as name and address. This information may be consumed by the email account management systems to give that student an email address based on their name, and the email address fed back into the SRS. Thus the email account management system is both a consumer of identity information – the student’s name – and an authoritative source of identity information – their email address.

7.4 Prioritising Targets

There are many different systems within an academic institution that an IdM solution could potentially be connected to. The integration of all of these is an end-goal of a long-term IdM strategy. Unless there are only a very small amount of systems, or staff within the academic institution have a great deal of experience with IdM, then a good method is to split this long-term strategy up into separate phases. How gradually this is achieved is a decision that needs to be taken by the institution. Slower is more likely to enable a successful IdM system, but means that benefits will likely take longer to materialise.

7.4.1 Identifying initial targets

The aim of a first phase of IdM implementation would be to establish the core IdM system and identity vault, connected to at least one data authority and one data consumer. This will allow identity data to be provisioned to the identity vault, and this information to be made productive use of by an identity data consuming system.

Getting this first phase implemented in a manner that is deemed successful by all involved is vital for the success of further phases of implementation. Any good experiences will help to achieve future stakeholder buy-in, while bad experiences may sour opinion on the IdM system and make further phases politically more difficult to achieve.

Which particular systems should be targeted can only be assessed within an academic institution however, the following general points can help identify which systems are most appropriate:

- Easiest to Accomplish
- Cost
- Co-operation of Vendor
- Standards
- Biggest Positive Impact
- Smallest Negative Impact
- Stakeholder buy-in

7.5 Writing an IdM Roadmap

The sections above describe how to work out what needs to be done, and how to organise it into phases. The final task is to turn this information into a draft Roadmap for IdM at the institution. To do this, it must be remembered that a Roadmap is not a Project Plan; it is a higher level strategy document, indicating projects which can be designed to fulfil parts of the Roadmap. This means that the most difficult tasks which face the author of a Roadmap is to give a timetable and estimated cost for the implementation of its phases.

If there are existing Roadmaps for other planned activities in the Institution, it is essential to consult these to see how the document can fit successfully into the local culture. Authors of these documents are also likely to be able to give good advice.

Once drafted, it is sensible to circulate and discuss the roadmap. An appropriate body to use for this would be the IT Service Management committee, or equivalent. Clearly, it will not be prudent to suggest major changes to systems which are due to be replaced immediately afterwards.

The Roadmap as described here is basically a one-off document. As an alternative, it is well worth
considering writing a Roadmap which is intended to be a rolling document, describing the next year’s work in considerable detail and outlining future phases to follow on from it, and then updating the Roadmap to reflect progress during this year.

The suggested main sections for the Roadmap are as follows:

- Introduction
- Requirements (or Problem Statements)
- Timetable
- Cost Estimates
- Staff Involvement

7.5.2 Roadmap Timetabling

Timetabling will consist mainly of slotting required tasks into each phase, and estimating how long each phase will take. As a general rule of thumb, each phase should last between 6 and 18 months; there may be local reasons to stick with a fairly rigid span for each phase (e.g. because matching a phase to a financial or academic year makes it easier administratively). If there are clearly related general institutional roadmaps already in existence, such as an IT Strategy roadmap, it will make sense to fit phases with the information in this and its update schedule.

As the Roadmap is going to include tasks which integrate different systems across the institution, the management team for each system will need to be consulted for timetabling work on it. They should also be able to help to estimate the time and cost of the type of changes that the Roadmap is proposing to make to these systems.

Each of the tasks listed for a phase would be a candidate for one or more IdM projects to carry out.

7.6 Conclusions

Establishing a roadmap for a measured, phased approach to implementing and maintaining an IdM system is vital if such a project is to be successful. Identifying which target systems should be integrated into the IdM system in which phase of implementation can be a major factor in this success, or in its failure. There are no concrete rules as to which systems, or types of systems are most appropriate; however, using the guidance provided should help an academic institution to make an informed choice and construct a roadmap that is suitable for their circumstances.

8 Ensuring Continuity of High Quality IdM

Work on Identity Management cannot stop once an institution has implemented high quality procedures and technical solutions. Institutional changes need to be reflected in the ongoing management of the policies and processes governing IdM.

There are various issues which can conspire to bring about a return to small scale ad hoc processes which reduce security and accountability, which are discussed in this section along with approaches which are suggested to help prevent the balkanisation of IdM in the institution. Methods which can be used to combat this problem include keeping a high profile for IdM in the institution, understanding how to apply IdM principles to new initiatives in the institution, and ensuring that members of the institution know about the local and global aspects of IdM as they apply to their role within the institution.

Effectively, the IdM roadmap needs to evolve into an IdM strategy, with IdM an important part of other strategic initiatives within the institution, becoming an automatic consideration when new projects are devised – in both teaching and research, and in the support services which enable these front line activities. Every new research project, every new application or service made available to users, every departmental re-organisation: all will have a role for IdM, and all carry the possibility of failure to maintain a sufficiently high standard to ensure security and efficiency for members of the institution.
8.1 Politics and the Profile of Identity Management

There is an important political role in promoting high quality IdM in an FHEI. Compared to many commercial organisations, FHEIs are often relatively anarchic places, with less scope for successful imposition of rules from the top of the organisation. However, it is still the case that without support from senior management, IdM will not get a place on many agendas at all. The business case for high quality IdM has been discussed elsewhere in the toolkit, and is a clear starting point for any attempt to maintain the profile of IdM, especially as anyone to be convinced of the need to promote IdM good practise will need to be convinced of its benefits.

8.1.1 What Happens When Identity Management is not on the Agenda

Essentially, the benefits of IdM practice are lost, as those involved in projects and the setting up of new services improvise their own IdM solutions independent of official services and processes. This is not because the people doing this would be unwilling to link to the official IdM infrastructure, but because they either do not know that it can work with them or because they want to do something which the official IdM infrastructure does not quite do, and either don't realise this or don't know how or expect it to take too much effort to request changes in the services and processes to cope with new use cases.

In the short term, connecting new projects and services with existing IdM processes and services may well take more work, especially if an external supplier has a product to sell which does not integrate with local IdM systems. It is important, therefore, to have some mechanism for both checking that this does not happen and helping those in situations where they have to work with unfamiliar services and systems, especially when they are the interface between the institution and a supplier. In this sort of situation, it is important that potentially complex local IdM requirements are not suddenly brought into play late in the day, but are established as early as possible; and this is impossible unless IdM is on the agenda in the institutional culture.

8.1.2 The Need for an Identity Management Strategy

In an FHEI, there are large numbers of people who can at least start a need for new services or initiate new projects. Students can bring pressure for such initiatives as Bring Your Own Device. Members of academic staff may want to start collaborative research projects with external partners, each participant needing access to local services in the institution. Support staff may need to establish access to new external resources, or seek to streamline physical access controls by introducing new management software and associated hardware. Changes in the law governing some aspect of the institution’s activities may lead senior management to enforce change within the institution, requiring, for example, new access restrictions on personal data.

All of these changes have IdM implications which need to be managed, and those involved in implementing these changes are the principal individuals who need to be convinced that existing central IdM processes should be used or modified as appropriate. However, these people, at the sharp end of changes, are not the only people who need to understand the requirements of IdM good practice, as they will need to have the time and resources to ensure that the new service or resource is integrated with existing systems and processes. This means that middle and senior management will need to be convinced as well, even though the actual knowledge they need will be less and of a rather different kind – business cases rather than technical details.

8.1.3 Formulating an Identity Management Strategy

To formalise the position of Identity Management in an institution, it is useful to produce an Identity Management Strategy. This will differ from the Roadmap because it does not have a specific, one-off target, but is designed to be a permanent and regularly updated document. The Strategy should start from where the Roadmap ends, on the assumption that most of the work described in the Roadmap has been carried out. But it will have similar aims (the promotion of good IdM practice) and a similar target audience, which means that the Roadmap would make a good starting point for development of the Strategy.

It may be considered appropriate for an IdM Strategy to be part of a more general strategic document, such as an IT Services Strategy. It should be remembered that the technical aspects are only a part of IdM, and that they are often easier to manage than the business processes and political aspects of IdM. IdM is also not restricted to a single department, but will be pervasive throughout the institution. For these reasons, it
makes sense to have a separate IdM Strategy, unless the culture of the institution seems to fit better with the idea of one which is part of an existing strategic document.

The Strategy should be a document which is regularly re-examined (say, once a year) and which has an owning body which meets regularly. The non-IT components of IdM make a IT Services committee a poor choice for this, especially as doing so would exclude important stakeholders such as HR and student administration. The appropriate group should be a cross-departmental committee of middle management with strategic responsibility, chaired by an appropriate senior manager.

The complete Toolkit proceeds to describe the contents of the major section in an IdM Strategy.

8.2 Applying Identity Management Principles to New Initiatives

As technology develops, and the roles of FHEIs evolve, the nature of IdM within the institution should also change. An institutional IdM Roadmap will need to develop to continue to be relevant. A large part of this work should be obvious, in that relevant new challenges to the institution are likely to be fairly widely discussed. However, it is important to undertake some analysis, even if at a fairly superficial level (e.g. during a meeting of the body which holds ownership of the IdM Strategy) to see what implications it has for IdM. In the main part, these are likely to be in three main areas: data management, privacy, and security. These are clearly related and will blur into each other for many developments; the way to think about them for this purpose is that data management is about storage of information and the related processes, privacy is about protecting the individual user, and security is about protecting the institution.

While it is possible to reduce the issues after the introduction of new developments, it is clearly better to influence the technology involved before the fact if possible. This can be done by:

- Ensuring that requirements in ITT documents include safeguards for security and privacy and only purchase systems which satisfy these requirements;
- Encouraging developers in house to include appropriate security and privacy safeguards in their software;
- Encouraging the development of APIs which have data security built in to their design;
- Designing policies and processes so that the introduction of new systems and services require thorough discussion of security and IdM requirements.

An example evaluation is discussed in a blog article evaluating the IdM implications of the consumerization of IT\(^6\), also known as Bring Your Own Device (BYOD).

8.3 User Communication

8.3.1 Introduction

Involvement of users in IdM is important, because without it they can be the weak link in security, through bad practice or lack of understanding what an institution is providing for them. So it is important to educate users in the best ways to use the IdM provided for them, and how to avoid security pitfalls. Related to this is the potential for members of an institution to use self-service IdM tools, of which there are potentially many kinds which could be made available, but all of which need some level of understanding of what is going on behind the scenes to be used effectively. As with every form of communication with users, it is important that what an institution tells them about IdM is accurate, clear, and helpful.

Social engineering – that is, persuading people to do favours which they should not do for someone they may well not know very well – is an important tool in the arsenal of those who have a serious desire to break the security of a computer system. Without user education on such issues as the undesirability of sharing passwords, an organisation is defenceless against this form of attack.

8.3.2 User Education

Keeping members of the institution informed about how central IdM at the institution is important for

\(^6\) http://theidentitytoolkit.wordpress.com/2012/08/02/identity-management-and-the-consumerization-of-it- services/
continuing to provide high quality IdM. Without information, members will start to improvise services of their own where the institution may well already offers such services (from setting up new facilities as part of research projects, to sharing of documents, to maintaining their own access control lists for items of equipment). This will eventually lead back to the chaotic situation where effort is duplicated and where services are offered which are insecure. There are basically two aspects to this kind of education: those which are institution specific, such as how to sponsor an associate member, and those which are general, such as how to choose a secure password.

**Institution Specific Education**

There are a variety of ways in which members of an institution interact with the institutional IdM processes. These include:

- being an end user of IdM, as one whose identity is managed (e.g. to gain access to the institutional network)
- being a consumer of IdM (e.g. as a developer wanting to add single-sign-on to an application being built)
- being a participant in IdM processes (e.g. as checking physical credentials such as a passport before assigning a userid)
- being an overseer of IdM (e.g. as the manager of MIS services)

Each of these relationships to the institution's IdM requires knowledge of, and (a variable degree of) understanding of the processes which have been put in place centrally to ensure its security and efficiency. Providing this knowledge and understanding is the role of institution specific education about IdM. However, it is also the case that different methods of imparting the education are appropriate to those who have these relationships. For example, end users can be informed about specific rules when they try to carry out an action which they are not permitted to do for some reason (e.g. attempting to log on to a server with restricted access which does not include the user), while training sessions could help consumers of IdM to be aware of central services which they can use, how to do so, and who to go to with problems.

Good practice in user education about IdM is essentially the same as that for communication with stakeholders in any business operation. The essentials of this are:

- Identify the stakeholders involved in the specific IdM change being considered correctly.
- Be clear on the aims of the communication exercise.
- Build trust with stakeholder groups (through competence, primarily, but also through openness and by demonstrating respect for the stakeholder). Accuracy in the information presented is vitally important.
- Listen to feedback from stakeholders before, during, and after the communications exercise (in a small scale project, the first two may not be appropriate).
- Act on the feedback as well as listening to it.
- Use a mixture of tailored methods to engage with stakeholders, where this is appropriate for the scale of the project.

**Generic Education**

Much of the information which institutions might wish to pass on to members is generic in nature, in that it will apply to members of organisations of comparable size to FHE institutions anywhere in the UK or around the world. This means that there are often very good resources already available on the Internet which can be used or adapted to impart such information to members, or which can help in the compilation of information to use (e.g. by helping the compiler to be sure that their advice is good and comprehensive).

**8.3.3 Assessing the Impact of User Education**

It is vital to measure the effectiveness of user education methods being used in an institution, to ensure both that the information is reaching the people who need to receive it and that money and effort is not being wasted on ineffective measures. A wide variety of methods can be used to make an assessment as to the
impact and success of user education initiatives. It can be possible to do so in the context of existing information gathering exercises, such as surveys carried out to assess the work of IT Services which many institutions carry out on an annual basis. As with the channels to use for user education, its impact is best measured by additions to existing tools to gauge the satisfaction of institutional members for the services it offers. For this reason, we will not give a list of possibilities here.

### 8.3.4 Self-service Identity Management

Many IdM systems have some form of self-service, where users can carry out tasks on their own behalf without having to involve central IT services staff. Giving users some control over their own data frees up the time of technicians who would otherwise need to make updates on behalf of users, though it can lead to problems if too widespread as there is little control if any over the quality of the data when updates are devolved in this way.

The integration of self-service consoles into a single portal, which can also be used for other services such as finance (e.g. employee expense claims, student fee payments, library fine payments) and library borrowing, is something which offers a unified interface which can be contextualised automatically to each user. This clearly improves usability, but at the cost of extra work to integrate services from disparate systems together.

As well as simplifying processes, self-service IdM encourages user involvement and provides an ideal channel for user education where it can be incorporated into help information and in checks made (e.g. by measures of password strength). All three of these are good reasons to adopt it for some processes, though a lack of full validation means that it is not appropriate for many types of data management.

### 9 Designing and Managing an Identity Management Project

This section deals with aspects of project management that may be particular to institutional work aiming to implement identity management facilities, including: Identifying the people to be involved in planning; Identifying the aims and scope of the project; Deciding on the approach to use; Integrating with non-IdM work; Assembling project plans and budgets. Common key institutional benefits of improved IdM are outlined for use in an institutional business case.

It is not possible for this Toolkit to offer a single business case, as institutional requirements and current positions will be very different, even if there are some gaps that are likely to be picked up by an audit. It is also the case that every organisation of the size of an FHEI will of necessity be carrying out IdM, so a business case for doing it is superfluous. This section describes, in general, how an IdM project could be designed and managed. It covers mainly those aspects of project management which are especially relevant to IdM work, rather than project management generally, which is covered by many books, articles and training courses. Institutions may have guidelines and policies covering project management (e.g. the use of frameworks based on PRINCE2 or other formal methodologies) which would be required background to the setting up of any project, not just an IdM project, and which cannot be covered here. This section will also not cover how to prioritise the different IdM projects which might be suggested by a Gap Analysis; this is covered by the IdM Roadmap section of the Toolkit.

The guidance given here is intended to be general enough to apply to IdM projects of any size, from small scale changes to data formats in an identity repository to the implementation of a central IdM system. Information specific to particular kinds of projects will be described in other sections of the Toolkit. No particular assumptions are made about the approach which is to be followed by the projects.

Similarly, the guidance here does not assume that the projects which are being designed are wholly, principally, or even tangentially technical IT work or, alternatively, concerned with business process management. Many IdM projects will be a mixture, and it should be remembered that implementing improvements to IT will not fix IdM issues where the underlying business processes are broken.

Key benefits from designing and managing internal projects to plug some known gaps in existing IdM processes will include:

- **Improved security**: Well designed, well understood, well documented and properly carried out IdM processes protect assets belonging to the institution.
- **Improved conformity with legal restraints**: Effective IdM processes will help prevent breaches of the Data Protection Act and of license agreements signed by the institution.
• **Improved efficiency:** Well organised IdM processes will prevent duplication of effort, and speed up processes such as user registration so minimising user frustration (e.g. with new staff members taking weeks to obtain working access to email). Well documented processes are easier to hand over to new staff, or to work with where the normal process management is unavailable. Well designed and properly implemented policies will ensure that management at all levels is able to obtain a good understanding of what the processes are and how they work. Projects which have IdM components (such as the introduction of new IT services which need to be integrated with an Authorisation Service) should be able to run much more smoothly.

This section will therefore suggest some generic components which can be used to produce a business case for an IdM project to fill a gap (or gaps) highlighted by a recently completed audit. By this point, it is assumed that an institution has carried out an audit or equivalent exercises to provide a gap analysis, so that there will be an individual or group of individuals with a good sense of where the gaps lie and what could be done about them. The content of this section will include both generic suggestions, effectively part of a business case for high quality IdM, and suggestions aimed at closing specific gaps and classes of gaps mentioned in the previous section. The audit report (and, if appropriate, information generated during the audit), together with the gap analysis, are likely to be vital sources of information for IdM related project design.

In particular, this means that no costings can be given, as the scope and nature of the project for which the business case is to be prepared is unknown.

It is also likely to be sensible to combine work on IdM improvements with other, related, tasks, such as enhancements to servers. This will often be necessary in any case, as security improvements may require software and configuration changes. In this case, the IdM enhancements should be included in a larger business case for the whole of the combined work, as this will tend to minimise risks and maximise benefits.

Managing change to business processes is often a difficult task, and when producing a business case for doing so, the author needs to be aware of potential difficulties which will be encountered. These tend to be political issues which are usually difficult to quantify in advance. Those who run processes may feel that they "own" them, and resent or fear changes made to them, and consciously or unconsciously sabotage projects which seek to alter the processes. Managers do not want to see crucial information moving out of the control of their team, particularly if their understanding of the replacement processes is kept vague. Those being assigned new processes may feel that they will now have too much work. These kinds of issues can only be solved by involving those who will be affected by change before the project begins: at the business case development stage, and by ensuring that all affected staff will be kept informed and/or involved throughout the proposed project.

The section ends with some guidance specific to particular types of IdM project, and a discussion of the appointment of staff to specific IdM management roles.

### 9.1 The Key Benefits of Good Quality Institutional Identity Management

It is worth describing the key benefits (listed above in the Introduction) of IdM improvement work in more detail. Many IdM projects will provide these key benefits to an institution, in varying degrees.

#### 9.1.1 Improved Security

Institutions have a duty to their members (staff, students) to manage data about them competently. This data itself has value, both to the member themselves and to the institution, and it can contain very sensitive information (such as bank account details). The value to the institution is such that it is impossible to function without it. Unauthorised access to, or loss of, or inaccuracies in, part of this data are all potential causes of problems with any process which uses this part. So it is vital that safeguards are in place to protect user data, both technical (e.g. the use of secure HTTP for authentication to web applications such as VLEs) and managerial (e.g. a procedure governing what information is permitted to be stored in mobile devices which may be stolen or mislaid off the institution premises). As the Privacy by Design report 7, published in 2009 by the Information Commissioner's Office, puts it: “Organisations use identity techniques to bind personal information to the individual: good approaches deliver greater anonymity and privacy for the individual, whilst poor approaches collect, duplicate and expose personal information.”

In addition to value in itself, user information is used to allow authorised access to other resources of value to the institution. This means that information made available to a third party could be used to gain

---

unauthorised access. Even where the actual credentials needed for access are not obtained by these third parties, the user attributes can often be used to obtain them (e.g. by providing information which can be used to guess poorly chosen passwords, or to persuade others to provide access when the third party poses as an individual who has lost their credentials through social engineering). Security breaches of this type will damage the reputation of the institution and may have legal consequences, as well as the direct losses which can be incurred when access is gained to physical and electronic resources (e.g. exam papers in preparation). Protecting sensitive user data is thus a form of insurance against potentially very serious security breaches.

9.1.2 Improved conformity with Legal Restraints

Institutions increasingly have legal constraints which regulate aspects of Identity Management. These are likely to include general legislative requirements such as the Data Protection Act, and requirements derived from agreements the institution has entered into such as resource licenses, federation membership agreements, partnerships etc. These will cover areas such as:

- how data is used
- publication of information about individuals (and when consent is required)
- accuracy of data about individuals
- prompt updating of data when necessary (including revocation of credentials when users are no longer entitled to hold them)

Clearly, it is essential for institutions to make their best efforts to comply with these constraints, and any work which is intended to improve IdM must as a matter of course look into what effect compliance will have on the desired outcome of a project. This should in turn mean that it is a priority to make sure that information on legal matters is available to those who might be designing and implementing IdM solutions; in some cases, such as with the multitude of resource licenses that an institution is likely to be a party to, this can be quite difficult in itself. It is likely to be useful to make an attempt to compile and maintain a list of known restrictions and access conditions which arise from sources such as resource licenses or Service Provider access conditions to help ensure compliance.

9.1.3 Improved Efficiency

Inefficient, poorly documented and duplicated business processes will be an unnecessary financial cost to the institution.

Loss of key members of staff who hold processes, policies and technical details in their heads is an unnecessary cause of disruption, which may have a high impact. Not only does it mean that their replacement needs to spend a great deal of valuable time working out how their predecessor carried out their tasks, but it leads to the invention of new processes, etc. designed in a hurry by someone not fully conversant with the institution and its idiosyncrasies. When a member of staff leaves, it is important to ensure that their job is documented, and if possible a hand-over period during which both the leaving staff member and their replacement are available (even if only electronically) is desirable.

Duplication of processes leads to wasted time and an increased potential for security problems. The latter is particularly likely to be the case if one of the processes is unofficial, and is carried out by someone lacking training in relevant subjects such as maintaining a data store securely.

Documentation is not enough to ensure high quality processes; there needs to be some assurance that the real life process matches (and continues to match) the documentation.

9.2 Designing an IdM Project

The following stages, most of which are going to be common to projects in any large organisation, may need to be passed through:

- Identifying the people to be involved in planning
- Identifying the aims and scope of the project
- Deciding on the approach to use
• Integrating with non-IdM work (if considered desirable)
• Putting together a project plan and budget
• Putting together a business case

This list is not necessarily chronological; indeed, the first four need to be at least considered more or less together as each will impact on the other three. The sensible way to approach this is to iterate through the first four until all those involved have common understanding of the basic project ideas, and then proceed to the business case, project plan, and budget.

Where there is an institutional roadmap for Identity Management, it is important that any IdM projects or project components are designed to fit in with the overall requirements of the roadmap; this will impact every one of these stages.

9.3 Managing an IdM Project

Once designed, an IdM project is likely to require similar management skills to any project. The major difference from work supervised by the project manager in the past (assuming that they are experienced in project management) is likely to be that the tasks involved will combine business process engineering with IT, and this is comparatively unusual. However, the design of the project is likely to have established the timetable, budget, risks, etc., and it is only the political elements which are likely to de-rail the process. This factor makes it unlikely that an inexperienced manager will succeed, except possibly in very small scale projects.

9.4 Appointing Staff to Manage IdM

It is likely that an institution will need to carry out several projects relating to IdM or that management will be needed to run central IdM systems which were not in existence or were not prominent beforehand. There are several roles which it may be appropriate to create, depending on the local circumstances.

9.4.1 Information Security Manager/Officer

This is a strategic post within the institution. The purpose is to mitigate risk within the institution relating to information, with respect to confidentiality, integrity, and availability.

Since IdM will relate to each of these aspects of information management, the post holder will have a significant interest in work on institutional IdM. The post combines technical input into IT developments (in particular relating to ISO 27000) with non-technical help on information risk management.

9.4.2 Identity Management System Manager

If a central IdM system is installed, then a permanent post should be established to manage it. The postholder will act to ensure reliable operation and continued enhancement to the system, in accordance with the roadmap or other relevant strategy documents and with guidance from (a group of) the IdM stakeholders who have already been mentioned in this section.

10 Selecting Supplier Solutions for Identity Management

Where commercial procurement of systems or components is required, this section aims to help understand the IdM system solutions available, produce procurement criteria, and construct tender documents. Issues of product capability, technical fit and vendor suitability are considered; and advice is given on specific aspects of a tendering process and phased implementation.

Once an academic institution has developed a programme of IdM work, and constructed a realistic roadmap for the work, the next step may be procurement of systems to achieve the initial goals of the roadmap. This section is designed to help academic institutions understand the IdM system solutions available, produce procurement criteria, and construct tender documents.

The IdM roadmap should inform several aspects of the process of choosing an appropriate solution for the

8  http://www.27000.org/
institution. It should:

- Indicate whether the preferred IdM architecture involves a central IdM system or working to integrate existing systems which handle parts of the IdM requirements of the institution (such as the Student Record System, the software used by HR and the finance department, and the mechanisms used to create accounts on various systems).
- Indicate how the IdM work that the institution is planning should be prioritised.
- Indicate general requirements for software solutions which need to be developed or obtained from a third party (whether a vendor or an open source development consortium).

The roadmap will be a top level solution, giving strategic information. The process which went into developing the roadmap, which may include a detailed IdM audit, will have produced more detailed analysis which should make it possible to turn the general requirements which can be seen in the roadmap into a collection of detailed requirements as would be appropriate for an ITT document or project plan (as appropriate).

### 10.1 IdM System Solutions

An IdM system solution aims to sit at the heart of the academic institutions, connected to each IT system, responsible for both various aspects of overall identity and account management and the connections into each IT system to manage their integration into this wider identity-driven ecosystem. This section refers to an "IdM System Solution" because a comprehensive IdM implementation is very unlikely to involve a single product, technology, or service. It will instead be an amalgam of various related elements that combine together to fulfil the IdM requirements of the academic institution. Which elements to use - and which products to chose that perform the tasks of that particular elements - may vary wildly between academic institutions based on their individual needs.

#### 10.1.1 Capabilities of an IdM Solution

While IdM implementations may vary wildly between academic institution, the whole solution of each will usually include at least the following main features:

- A central repository of identities and related identity information;
- Synchronisation mechanisms to various applications - to be able to "talk" in multiple protocols or languages to a variety of applications, enabling the gathering and publishing of identity information;
- Account provisioning/de-provisioning abilities - to control access for individuals within connected IT systems by provisioning/de-provisioning accounts within these systems and by managing those accounts' rights based on identity information.

These features provide the core functionality required of an IdM system solution. Beyond these, many other features are often seen. These may include, but are by no means limited to:

- Auditing - to provide comprehensive change history;
- Directory - to use as an Authentication back-end and to supply attributes used for Authorisation.
- Federated Identity Provider - to enable authentication and authorisation to remote services via federated means (e.g. using SAML);
- Group Management - to enable automated and/or manual placement of users into groups (useful for authorisation decisions);
- Identity reconciliation - automated and/or manual mechanisms for taking existing accounts from multiple IT systems and identifying, to a certain degree of probability, that those accounts belong to a single individual and linking them within the central identity repository;
- Password management - to enable password synchronisation between IT systems, enforce global password policy across these systems, etc;
- Self service portals - to allow individuals to update their information without the need of going through a central administration point;
• Shared Authentication Service - to allow seamless access to a variety of systems with a single credential;
• Workflow - to allow change requests of various natures to be submitted, validated, verified and approved by specified authorised personnel, and automatically actioned.

10.1.2 IdM Products

Many products are available in the marketplace that offer the core functionality of an IdM System Solution as outlined above, along with many of the other features discussed. Some examples of these products are those available from large well-known vendors - such as CA, IBM, Microsoft, Novell, and Oracle - and those from more specialised players such as Courion, Avatier, and many others. Sources such as Gartner can help identify these available products.

Many products from the larger vendors exist as a part of a vertical stack of applications that together provide most or all features potentially required for IdM, security management, legal compliance, auditing, single sign on, and a host of other related features.

A general comparison between IdM products is not feasible - genuine informed comparisons can only be drawn given a specific set of circumstances to calculate which is the most appropriate. However, some technical considerations for comparing IdM products and some general considerations to take account of when choosing the correct product for an academic institution can be detailed, and are presented next. Additionally, some of the questions presented in the Identity Management Policy Checklist Appendix may be of use in this task.

10.1.3 General IdM Software Considerations

There are also many general aspects relating to IdM products that should be considered when performing a comparative evaluation of them. This section lists some of these aspects; more details are given in the complete Toolkit.

• Technical Appropriateness
• Cost
• Flexibility
• Maturity
• Scalability
• Security
• Data Storage (and the Cloud)
• Outsourced/Third Party Identity Management (Identity as a Service)
• Open Source Identity Management Systems

10.1.4 Vendor Considerations

There are several aspects relating to vendors who may bid on a tender issued by an academic institution. This section lists some of these aspects that should be considered when selecting an appropriate vendor; more details are available in the complete Toolkit. Note that some of these are very similar to the considerations discussed around the vendor of the IdM products as previously discussed, since many of the issues are similar in nature.

• Existing Academic Customer Base
• Partners
• Vendor Stability
• Support
10.2 Tendering

Given the highly specialised knowledge often required when implementing IdM system solutions and their connection to existing applications, the detailed analysis, specifications, and technical implementation of many large IdM implementation projects is often procured externally from the academic institution itself. This section provides some help and guidance around how this procurement could happen.

Since an IdM system is such a fundamental and far reaching system, any procurement is likely to be on a not-insubstantial scale. Since academic institution are generally public sector bodies, then various parts of EU procurement law may come into play. Academic institutions will need to ensure they abide by these laws at all stages.

The implementation of an IdM system can be a long term process made of many disparate projects, each with their own requirements and budget. The initial project, however, should have a fully defined budget from its very beginning.

There are many possible approaches to the organisation of the implementation of an IdM system. Which approach is used, and how it is used, will depend on what best fits the academic institution, circumstances, and budget.

Essentially, the implementation of an IdM system can conceptually be split into two separate phases:

Phase One – The drawing up of a detailed specification of hardware and software required, and a detailed project plan for implementing these;

Phase Two – The actual implementation of the system(s) detailed in Phase one, including testing, documentation, and migration of existing data.

One recommended implementation possibility is that of using a two phased approach, where each phase matches the conceptually disparate phases detailed above. Each of these phases, and how they can be organised, are discussed next.

10.3 Conclusions

The procurement and implementation of an IdM system solution - consisting of an amalgam of various related elements that combine together to fulfil the IdM requirements of the academic institution – is a highly important part of any IdM implementation. Choosing a set of products and elements that fit the current needs of the institution and that are flexible enough to meet future needs, and working with vendors that offer the support required, can drastically increase the chances of a successful IdM implementation. Choosing the wrong products and elements can doom such an implementation to failure.

No concrete advice can be given on which IdM products are the “best”, since they all have comparative strengths and weaknesses that can only be understood given a specific set of circumstances. However, following the general advice given in this section, and working in close partnership with vendors and external consultants with a good deal of domain knowledge, can help an academic institution make informed choices as to which set of products and elements making up an IdM system solution is the most suitable for them.

Appendix: Identity Management Glossary

This list is not intended to be exhaustive but contains terms and abbreviations used in IdM, and in other sections of the Toolkit, and their meanings in an IdM context.

API

Abbreviation for “Application Program(ming) Interface”. The API for an application defines the methods which other software (possibly including non-local software using the Internet for access) can use to interface with the application, defining conventions and vocabulary for this purpose.

Asset repository

A database in which physical and virtual resources are modelled, used to define and manage access to these resources. Typical resources will include rooms, and the database will define who can enter them, who can book them, etc.

Attribute
A single piece of information about an individual, which may take multiple values. Examples include userID, eduPersonEntitlement, telephone number. Usually aggregated into schemas, particularly in the LDAP context. Attributes are usually stored in a database (sometimes known as a directory), but may also be determined by the user or generated by an identity provider.

**Authentication**
A process by which an individual proves their identity, particularly electronically. (A common abbreviation for this is AuthN)

**Authorisation**
The process of determining whether an individual is permitted a level of access to a resource or part of a resource. (A common abbreviation for this is AuthZ)

**Certificate**
An electronic document which is bound to an entity, such as a server or an individual and can be used to verify their identity. A form of credential.

**Credential**
Data which can be used to verify the identity of an individual. Common forms of credential include usernames/passwords, certificates, and documents such as passports.

**Customisation**
The process whereby an individual can determine some of their own attributes rather than using values obtained from other sources such as the institution of which they are a member.

**Directory Access Protocol (DAP)**
Protocol used to access a directory service. The most popular of these is LDAP.

**Directory service**
An interface to a database which stores attribute and security information for a number of users. Often used as an Authentication back-end and to supply attributes used for Authorization.

**eduRoam (formerly Janet Roaming Service)**
Service enabling visitors to participating organisations to use their home network credentials for access (if their home institution is also a member). See [http://www.ja.net/services/authentication-and-authorisation/janet-roaming.html](http://www.ja.net/services/authentication-and-authorisation/janet-roaming.html). Extends beyond the UK through international partnerships.

**Expiry**
A built in end date/time to the validity of a credential.

**FAM**
Abbreviation for "Federated Access Management". Method of providing authenticated access to electronic resources where the authentication is separated from the resource. The authentication system is known as the "identity provider", and the resource protection system is the "service provider", and access is granted on the basis of attributes about the user passed from the identity provider to the resource provider.

**Federation**
In Federated Access Management, a federation is a group of service providers and identity providers which agree to share trust information, and commonly also common standards for attribute usage.

**Identity audit**
Comprehensive investigation into the business processes and technical systems used to manage identity in an organisation. See detail in audit section.

**Identity management**
Briefly, the processes and systems that allow the creation, retrieval, update, verification and destruction of identities and information relating to identities including any rights / authority granted to the identities. A fuller discussion is found in the definition section of the toolkit.

**Identity provider**
In Federated Access Management, the system which handles user authentication and provides attribute information about the user to the service provider. Usually connects into other systems, such as a directory service.

**Identity repository**
Database where identity attributes are stored, and tools which allow creation, updating, activation, suspension, de-duplicating, archiving, deletion and restoration of user accounts. Machines or services may also have an identity. A fuller discussion is found in the definition section of the toolkit.

**Identity vault**
A directory which contains information central to a variety of other directories, with the aim of managing the flow of data between directories and improving data quality through deduplication and the reduction of incompatibility between attributes stored in different directories. Some IDM software uses a relational database for this instead of a directory.

**KR**
Abbreviation used in this toolkit for "key researcher", the main individual tasked with carrying out an institutional IdM audit.

**LDAP**

**Metadata**
Information describing the properties of an object. In IdM, this is often a person (in which case it would be "user metadata").

**Password**
A short hidden or encrypted piece of text used to verify the right to a userid for identification of an individual. Together with the userid, this forms a type of credential.

**Personalisation**
The targeting of service delivery to individuals based on their attributes. (This may include information provided directly by an individual to the service.) Examples could include highlighting of information deemed relevant because of departmental membership, or use of a preferred language.

**Portal**
A website which provides access to information stored in a variety of locations. A portal often needs to act as a proxy to other services, so that users can authenticate to the portal and seamlessly view the information without further sign on.

**Proxy**
(1) A service which can present credentials to other systems on behalf of logged in users without the users concerned needing to authenticate to these other systems directly. (2) A user who is entitled to perform actions formally restricted to another on their behalf (e.g. as a PA, or to fill in during absence).

**Revocation**
The enforced expiry of a credential, e.g. by the body which issued it in response to loss or misuse.

**SAML**
Security Assertion Markup Language. A standard which describes methods of passing security information online. Used by several FAM applications including Shibboleth to obtain access to resources for users.

**Schema**
Generally a definition of a database structure. In Directory Services, it is the definition of a set of attributes and classes often for a specific purpose. The eduPerson schema, for example, is used to store attributes of students and related objects.

**Service provider**
In FAM, the subsystem responsible for the protection of resources. A service provider should allow access dependent on information provided by a trusted identity provider, and prohibit access when this information is incorrect or absent.

**Shibboleth**
FAM software widely used within the UK Access Management Federation.

**SRS**
Student Record System. Identity repository which is generally the authoritative source of data for students and their interaction with the institution.

**SSO**
Single Sign On. Technology which (in simple terms) allows a user to log on once and thenceforward have access to all the resources to which they are entitled without being challenged for credentials again. In practice, a variety of different levels of SSO are usually available.

**UK Access Management Federation (for Education and Research)**
Organisation of Identity Providers and Service Providers using FAM in the UK.

**userid or username**
A clear text indication of a user's identity, used in partnership with an encrypted or hidden password as a credential.

**Virtual Organisation**
A group of individuals who share common goals and who pool resources, such as a research group or study partners. This definition matches pretty well with Wikipedia's virtual enterprise[^9].

**WAYF (Where Are You From service)**
FAM component allowing users to choose the Identity Provider which they will use to authenticate to a Service Provider.