Federated access management: institutional business case toolkit

Federated access management:

institutional business case toolkit

CC297D001-1.0
10 July 2007
Cover + 74 pages

Dr Claire Davies
Matt Shreeve

Curtis+Cartwright Consulting Limited
Main Office: Surrey Technology Centre,
Surrey Research Park, Guildford
Surrey GU2 7YG

tel: +44 (0)1483 295020
fax: +44 (0)1483 295021
email: postmaster@curtiscartwright.co.uk
web: http://www.curtiscartwright.co.uk

Registered in England: number 3707458

Registered address:
Baker Tilly, The Clock House,
140 London Road, Guildford,
Surrey GU1 1UW

Key points

A changing landscape

1 The access management landscape for education and research is undergoing significant change within the UK and the rest of the world. New technologies and services are available to protect electronic resources and services. Universities and colleges need to determine how they will address these changes and opportunities.

2 Access management covers providing appropriate access to the full breadth of protected resources and services including, but not limited to, internal services such as VLEs, email and corporate systems, external licensed resources, and collaborative tools such as inter-institutional repository sharing and Grid computing.

A range of options

3 A range of options is available to institutions and a choice is required. The choices include whether to adopt federated access management and whether to join the UK Federation. It is not just a decision whether to subscribe to Athens after July 2008 or whether to deploy Shibboleth technology: there are broader strategic questions, and additional operational options, to consider.

4 Institutions can choose how much change they want. If limited change is desired then only operational decisions are required. It is not the intention for any institution to lose out, though some understanding and action is necessary.

5 Experience has shown that it is necessary to include senior management from both IT and Library Services, and other key stakeholders, early on in the decision-making process with clear assignment of responsibilities.

Adopting federated access management

6 There are significant potential benefits of federated access management if adopted fully, though the accompanying business change will be considerable, particularly for diverse and more complicated information environments. Adopting may not be the right option for every institution.

7 Realising the benefits of federated access management requires an institution-wide business change project rather than a technology project. Fully adopting will be difficult and depends on infrastructure and policy that may, or may not, already be present. An in-depth understanding and a strategic decision is advised in this instance.

8 Access management relies on effective identity management. A good understanding of requirements and current practice of both are necessary for federated access management.

Using this toolkit

9 This toolkit aims to support better and more appropriate decision-making by providing a process to follow, and guidance in key areas. Strategic issues are discussed in Section 3 and the benefits, costs and risks of various choices are set out in Section 4. Four case studies are referenced to inform decision-making and lessons from early efforts are set out to highlight good practice.

10 Annex A (page 65) provides a checklist of questions to consider when making a choice.

This page is intentionally blank

List of contents

List of abbreviations

ADFS	Active Directory Federated Services
AY	Academic Year
CM	Core Middleware
FE	Further Education
HE	Higher Education
ICT	Information and Communications Technology
IDM	IDentity Management
IdP	Identity Provider
INSRV	INformation SeRVices
IT	Information Technology
JISC	Joint Information Systems Committee
MIS	Management Information System
OGC	Office of Government and Commerce
R&D	Research and Development
SAML	Security Assertion Markup Language
SP	Service Provider
TCO	Total Cost of Ownership
VLE	Virtual Learning Environment
VRE	Virtual Research Environment

This page is intentionally blank

1 Introduction

1.1 General

1.1.1 The access management landscape for education and research is undergoing significant change within the UK and the rest of the world. New technologies and services are available to protect electronic resources and services. Universities and colleges need to determine how they will address these changes and opportunities.

1.1.2 The development of a new and federated access management infrastructure in the UK has been embodied by the launch of the UK Access Management Federation for Education and Research ("the Federation") by the Joint Information System Committee (JISC).

1.1.3 The JISC is supporting institutions adopting federated access management. All UK FE and HE institutions have options to consider regarding their access management strategy and operations; this business case toolkit provides guidance to support the decision-making process. This is a strategic-level decision, particularly where underlying processes and systems are affected, for example those concerning identity management.

1.2 Aims

1.2.1 This business case toolkit aims to:

- enable an understanding of the potential benefits, costs, risks and timescales of top-level options for access management strategies and operations;
- support better and evidence-based decision-making and implementation by using a clear process and applying lessons from others.

1.3 Scope

1.3.1 This toolkit supports UK FE and HE institutions that need to make access management decisions.

1.4 Audience

1.4.1 The toolkit is intended to be read by relevant senior managers and their support staff. Experience has shown that it is necessary to include senior management from both IT and Library Services, and other key stakeholders, early on in the decision-making with clear assignment of responsibilities.

1.4.2 Service providers also need to consider their strategies and approaches, though this toolkit is not designed for such guidance.

1.5 Context

1.5.1 Access management covers providing appropriate access to the full breadth of protected services[1] including, but not limited to, internal services such as VLEs, email and corporate systems, external licensed resources, and collaborative tools such as inter-institutional repository sharing and Grid computing.

1.5.2 In November 2006 the JISC launched the Federation. Universities and colleges throughout the UK are invited[2] to join and adopt new technology such as Shibboleth.

1.5.3 The existing Athens system will be available via a subscription service within the Federation from August 2008. The JISC will not be funding Athens from this date and all institutions using an outsourced identity provider, like Athens, will need to subscribe.

1.5.4 The JISC ran two development programmes between April 2004 and March 2006 to plan and prepare for the new infrastructure. These Core Middleware programmes (CM programmes) established the early elements of the infrastructure and generated lessons for institutions in the future. The CM programmes covered internal, third party, inter-institutional and *ad hoc* collaboration uses of federated access management.

1.5.5 The JISC has established a transition programme with clear choices for institutions, and has produced a six-stage roadmap for institutions and service providers that outlines these choices.[3] The first step on the roadmap is an institutional audit to review readiness to adopt federated access management. This includes making a choice of access management strategy and alignment with institutional information strategy. This toolkit provides advice and guidance for carrying out the institutional audit.

1.6 Is this a strategic-level decision?

1.6.1 The move of Athens to a subscription service may not, in itself, be a strategic issue for many institutions. New technologies and services can be reviewed and dealt with at an operational level. It is advisable to ensure that these decisions are aligned with existing access management strategy.

1.6.2 Many institutions will have heard of different operational and technical options, such as OpenAthens and Shibboleth. These are not the only options; there are other technical options (*eg* those based on ADFS[4] and GuanXi[5]) and many ways in which these technical options can

---

1 The (concise) term "services" is used here over the traditional term "electronic resources and services".

2 The announcement and invitation from the JISC Executive Secretary for federated access management and the Federation can be found at <http://www.jisc.ac.uk/uploaded_documents/Shibb-institution-letter.pdf>.

3 The JISC roadmap for joining the Federation can be found at: <http://www.jisc.ac.uk/media/documents/publications/fam leaflet final.pdf>.

4 See, for example, the Microsoft website on Active Directory Federated Services (ADFS) (<http://www.microsoft.com/windowsserver2003/techinfo/overview.mspx>) and recent work between Microsoft and the education and research sector in *Achieving Interoperability between Active Directory Federation Services and Shibboleth*, Microsoft Limited, January 2007.

5 GuanXi is an implementation of the Shibboleth profile, funded by the CM programmes.

be used to deploy federated access management. Experience has shown that technical issues are only part of a broad picture: considerations such as support, business change, *etc* might prove to be more important.

1.6.3 However, choosing an approach may be a strategic-level concern due to issues such as the changing access management landscape, questions over identity management and single sign-on and other strategic drivers. This toolkit supports good practice, strategic and senior decision-making relevant to federated access management.

1.7 Why prepare a business case?

1.7.1 All UK FE and HE institutions will need to make decisions regarding their approach to management of access to protected services. Research shows that although some already have decided, many have not.[6] A business case is a means of weighing up various options and making and recording a decision. In some instances, this decision will be relatively straightforward; in others it will be difficult and require justification to a governing or funding body. In any case, it is important for the institution that the right choice is made.

1.7.2 Developing a business case forces a well-considered decision that assesses a range of options. Managing a business case throughout an undertaking supports successful implementation by keeping activities "on course" for the desired outcome.

1.7.3 Business cases for infrastructure projects, like ensuring appropriate and secure access management, are often difficult to write. Because they only enable further activities they do not provide the immediate end-benefits that, say, a new finance system or messaging service might. Developing a business case will allow consideration of these issues, and how any new investment compares with other institutional priorities.

1.7.4 Good practice is for the senior manager or management team responsible for access management to develop and then manage the business case. Experience shows that well-managed business cases support successful outcomes and realisation of benefits. In short, the value of a properly written and managed business case stems from:

- presenting and communicating the rationale for an undertaking;
- presenting the big picture to the rest of the institution within a single point of reference;
- permitting performance management by setting out benefits and envisaged outcomes;
- providing an auditable trail for accountability.

1.8 Approach taken by the toolkit

1.8.1 UK FE and HE institutions are tremendously diverse. As each institution is different, generic guidance or a "one size fits all" approach is neither feasible nor desirable. This toolkit of guidance enables institutions to make decisions that are appropriate to their own

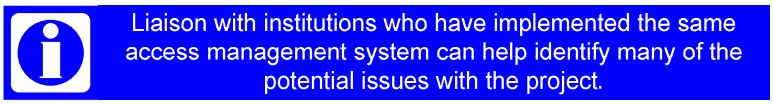
6 *Federated access management: institutional preparedness study*, CC273D001-1.0, Issue release 1.0, 5 December 2006.

circumstances by covering a range of exemplar options but not promoting any one as the "answer".

1.8.2 Access management strategies and operations in this context cover a vast range of activities, from setting up a subscription, introducing and running a new system, through to transforming identity and data management within an institution. Technical changes and business process changes may be required depending on the option and mix of activities. This toolkit focuses on key access management decisions, setting out context and assumptions when required.

1.8.3 Although this toolkit sets out a formal process for making access management decisions, it is acknowledged that formal business cases may not be part of an institution's decision-making and governance processes. Where this is the case the toolkit can be used as an aide to exploring the issues and considerations that should be taken into account within whatever process is used to make and review these types of decisions.

1.8.4 The framework within this toolkit is based on business case best practice provided by the Office of Government and Commerce (OGC).[7] The framework is populated by relevant questions, information and lessons from UK and international activities from the access management arena. Lessons synthesised from the CM programmes are grouped together and referenced in Annex C, and are highlighted within a blue information box, like the following:



1.8.5 This toolkit is supported by a supplement[8] which presents a series of detailed institutional case studies providing further "real world" insight. The case studies consider four institutions that have the experience of going through the choices. They are introduced in Figure 1-1, overleaf.

7 See <http://www.ogc.gov.uk> for business case and other areas of best practice guidance.

8 *CC297D002-1.0 federated access management: case studies supporting the business case toolkit*, 10 July 2007.

Cardiff University

Cardiff University is a large institution comprising approximately 5,000 staff and 18,000 students spread across 28 academic schools and 5 administrative directorates. It has close links with NHS Wales.

The main aim of the project was to implement Shibboleth technology as a replacement for the extant Classic Athens access management system in conjunction with funding received from the JISC as an Early Adopter of Shibboleth technology.

The project was carried out by Cardiff's Directorate of Information Services (INSRV), which aims to deliver superior computer, library and media services that make a distinctive contribution to CU's research, learning, teaching, community activities and administrative functions.

Kidderminster College

Kidderminster College is a small college in the West Midlands, supporting approximately 5,100 students, of which 1,000 are full-time. Kidderminster offers a wide selection of full-time and part-time courses lasting up to 2 years.

The main aim of the project was to implement federated access management using Shibboleth technology within Kidderminster College to link together web-based resources.

The project was carried out by the Development team within ICT Services. Kidderminster, unlike many FE colleges, has a dedicated IT development team that does not have a support remit. The ICT Services Development team is well resourced, well trained, proactive and confident with open source software.

University of Surrey

The University of Surrey is a moderately large campus university, supporting approximately 18,500 users. It has an institution-wide policy to implement mature commercial systems and has a very lean staffing structure.

The main aim of the project was to replace the Classic Athens access management system at Surrey and to implement a devolved authentication system in order to reduce the administrative burden on IT staff.

The project was carried out by the Library and IT Departments which are separate but under the joint remit of the Director of Information Services. IT Services to provide a high quality, user focused IT service that meets both the academic and business needs of the University.

University of Warwick

The University of Warwick is a large institution comprising of approximately 5,000 staff and 16,000 students. It has five main schools, including Warwick Business School.

The main aim of the project was to upgrade the extant access management system (for access to web services) at Warwick to improve its security.

The project was carried out by Warwick's E-lab, the development division of its IT Services. It has teams covering web services, e-learning, projects development and business systems. Its purpose is to provide a focal point for development, especially work relating to the web.

Figure 1-1: institutional case studies

1.9 How to use this toolkit

1.9.1 This toolkit is best used prior to committing to a way forward, thereby contributing to informed decisions. If required, the document structure can be used to write a business case setting out the rationale for the way forward.

1.9.2 Relevant background information is set out within Section 2.

1.9.3 It is necessary to identify access management requirements prior to working through the toolkit. A top-level set of common requirements is provided at Annex B.

1.9.4 The main body of this toolkit provides the questions and guidance to decide access management strategy. The toolkit comprises the following steps:

a) **Strategic fit**: identifying strategic issues and drivers for access management (Section 3).

b) **Options appraisal**: considering the range of access management options available and conducting an options appraisal to identify which option best meets the business need (Section 4).

c) **Affordability**: assessing the affordability of the option identified by considering available funding, existing commitments and estimating whole-life project and operating costs (Section 5). Where the identified option requires an external procurement, the commercial arrangement should be assessed to ensure value for money can be obtained (Section 6).

d) **Achievability**: assessing the achievability of the option identified, within current capability and capacity and the intended business change (Section 7).

1.9.5 Some readers will find following the steps a valuable and comprehensive process that identifies and justifies an access management strategy; others will find that it raises issues and provides lessons within their own process. Since the answers to questions posed within the toolkit will be different for each institution (due to drivers, priorities, different legacy systems, *etc*), the experience will be unique for each institution.

1.9.6 Decision-making is best conducted initially at a strategic-level to identify the top-level option for the way forward. There will likely be a requirement to conduct subsequent analysis to enable decision-making at a more detailed level, for example to determine the exact implementation specifications of the chosen option.

1.9.7 A diagrammatic representation of the framework is provided at Figure 1-2, and a checklist for the toolkit is provided at Annex A.

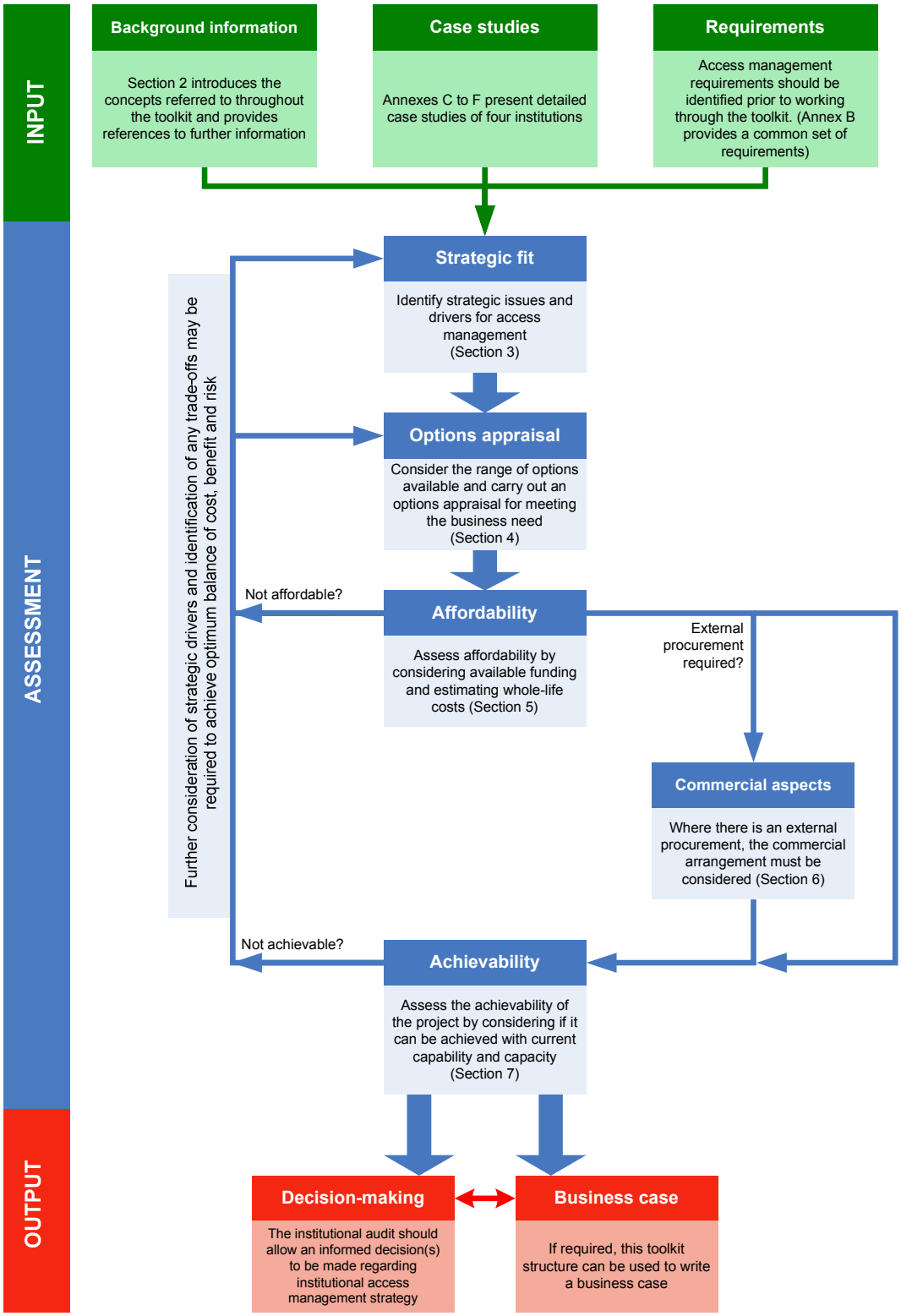


Figure 1-2: how the toolkit can be used to make an informed and appropriate decision on access management strategy

1.10 Moving from decision to implementation

1.10.1 Once a top-level option has been chosen, further analysis can be conducted to select an implementation option. Good practice is to move from a more strategic view to a more detailed view though, of course, successful projects can expand and become a larger and more strategic change than originally intended.

1.10.2 This toolkit does not detail the range of implementation options but provides a link between these stages of planning. Again it is worth noting that the process is iterative; revisiting decisions when faced with new information or when additional detail is available is normal.

1.11 Further information

1.11.1 There is an increasing amount of literature available supporting the access management landscape. Notable specific sources are referenced throughout the toolkit as required. The key sources are:

- the JISC's website dedicated to helping institutions and service providers in their transition to federated access management <http://www.jisc.ac.uk/federation>;
- the Federation's website that details the joining process and provides guidance on the technical aspects of federated access management <http://www.ukfederation.org.uk>;
- the Athens service website <http://www.athensams.net>.

2 Background

2.1 Introduction

2.1.1 There is already a range of briefing and background material on federated access management and related concepts.[9] There is also expanding guidance on the standards and technologies that be used at a more technical level.

2.1.2 This section answers some background questions and sets out an overview of the relevant concepts and terminology used within this toolkit. It is not intended to be a full or comprehensive guide, and some prior understanding is necessary.

2.2 What is access management?

2.2.1 Access management is the term used to describe the process of permitting access to protected online information, usually in the context of web pages or web-based applications. These might include services such as VLEs, electronic resources (including those currently protected by Athens, and those not), webmail, library portals, *etc*.

2.2.2 Access management is part of the process of connecting people to services. It describes both the means by which a web-based service decides and allows access to a protected service, and also the administrative process of allowing access for approved individuals.

2.2.3 Access management can also be used in other contexts such as non-web-based databases and applications, network and computer log-on and non-user level services such as directory services. The scope of the toolkit can encompass these contexts as well as they can be viewed as services, though often additional effort will be required to integrate these into an access management infrastructure.

2.2.4 Services are protected by access controls: authentication mechanisms normally using credentials (*eg* passwords or digital certificates) and authorisation by technical "deciders" and "enforcers".

2.2.5 The way in which access controls are used to implement institutional policy is important, determining processes for managing credentials; user experiences (as the gateway, or barrier, for accessing and using services) and security.

2.3 What is federated access management?[10]

2.3.1 Federated access management builds a trust relationship between identity providers (commonly termed "IdPs") and service providers ("SPs"). It devolves the responsibility for authentication to a user's home institution, and establishes authorisation through the secure exchange of identity information (termed attributes) between the two parties. Service

---

9 See, for example, the JISC briefing paper explaining what Shibboleth is and its consequences (<http://www.jisc.ac.uk/uploaded_documents/JISC-BP-Shibboleth-v2-final.pdf>) and the Federation's Rules of Membership (<http://www.ukfederation.org.uk/library/uploads/Documents/rules-of-membership.pdf>).

10 The JISC have produced an animation explaining the concepts and significance of federated access management. This is available at <http://www.jisc.ac.uk/whatwedo/themes/access_management/federation/animation.aspx>.

providers may be internal (*eg* IT Services providing a VLE, or Library Services offering a portal) or external to the institution (*eg* another institution or a third party).

2.3.2 Service providers trust institutions to authenticate their users and to provide the correct attributes in response to their requests. The objective is to ensure that a user cannot access a service to which they are not permitted under the relevant terms and conditions of the service. Institutions trust service providers to provide access to users when authorised according to the relevant terms and conditions.

2.3.3 A federation is a group of institutions and service providers that sign-up to an agreed set of policies for exchanging attributes about users to enable access and use of services. The federation therefore acts as trust "broker" to create the necessary trust relationships for this type of access management to work. Many types of federation with various policies are possible, for example at regional, national or international levels.

2.3.4 In this context, federated access management differs from centralised access management because there is no centralised authentication or authorisation service, only a federation that enables and records agreements between institutions and service providers.

2.4 Why is the JISC supporting federated access management?

2.4.1 Devolved authentication as a principle, and open and international standards in implementation, are considered significant advantages for federated access management.

2.4.2 Devolved authentication gives control of identity information to institutions, who know their users better than a third party. Administration and release of information can be better controlled.

2.4.3 Open and international standards are at the heart of the federated access management initiative. Open technical standards and technology and international uptake are considered strategically beneficial and support a global access management infrastructure within the education and research sectors. For example:[11]

- The Security Assertion Markup Language (SAML) is an open, flexible and extensible standard that facilitates the exchange of identity information. SAML has gained widespread industry adoption as a basis for federated identity and security environments and can be applied in a number of ways.

- The Shibboleth profile is a SAML profile that separates authentication and authorisation for an open, loosely-coupled approach to access management between institutions and service providers.

- There is a new and rapidly growing international community in which the concept of federated access management is generally embedded. There many national federations in production and others in development. International service providers, international consortia and major computer technology vendors are also major contributors.

11 *Federated access management: international aspects*, CC253D018-0.2, March 2007.

2.4.4 An access management infrastructure is also considered to facilitate collaboration, for instance inter-institutional content sharing.

2.4.5 Supporting federated access management within the UK is part of the JISC's mission to provide world-class leadership in the innovative use of information and communications technology in education and research.

2.4.6 Athens will continue to be funded by the JISC until July 2008. It is the JISC's strategy to move "mature" services towards sustainable models in order to release core JISC funding for innovative services. In this case, the sustainable model for Athens is a subscription model, and the innovative services are the Federation's services and the emerging federated access management infrastructure.

2.4.7 Athens will be part of the federated access management infrastructure in the UK, with the OpenAthens range of offerings to institutions and service providers. These mostly concern third party, licensed resources and services. Interoperability within the infrastructure is being provided by gateway interfaces that are funded by the JISC until at least July 2008.

2.4.8 The launch of the Federation and decision to move Athens to a subscription service followed the CM programmes which, as part of JISC's development activities, explored and piloted the technology through implementation by a range of institutions and service providers.

2.5 What is the role of identity management?

2.5.1 Access management seeks to address one question each time a user tries to access a service: is this user permitted to access this service? The answer relies upon the identity of the user and their entitlements. Sometimes, individual identity is required (*eg* access to user accounts) and sometimes not (*eg* where access is permitted for all institution members, and denied to those that are not). Sometimes identity must be extended to include other parameters, such as the location of the user (*eg* where access is granted to anyone on-site, and denied to those that are not).

2.5.2 User identity, defined as "the characteristics of the fact of being who a person is", is an aggregation of the information known about each user. Institutions will record much identity information, but third parties, such as service providers, are likely to as well. Institutions themselves also have an identity, used (perhaps through an empowered representative) and expressed in legal agreements and, in federated access management, within trust agreements with service providers.

2.5.3 Identity management is the term used to describe the institutional processes of recording, maintaining, using and retiring identity information on users. It includes account provisioning and deprovisioning, and the ongoing management of user attributes, entitlements and credentials.

There is often no clear owner of the identity management problem within institutions. For institutions with such owners, there is little consistency in their position or role. This can be an issue with addressing identity and access management.

2.5.4 Effective identity management means complete, consistent and timely processes for managing and using identity information:

- Complete means all users are included (staff, students, visiting academic staff, contractors, alumni, walk-in users, honorary members, *etc*) and all types of identity information required.
- Consistent means data integrity and conflict-free identity information.
- Timely means accurate identity information that is available and up-to-date at the time of need.

2.5.5 Ensuring that someone is responsible for identity management can be critical. Very often it will be a strategic issue and an appropriately senior owner of the issue will be beneficial. Responsibility for identity management may not be best located in IT services as it requires a detailed understanding of many institutional business processes.

2.5.6 Identity management is a "live" topic within institutions and is expected to grow in importance.[12]

Cardiff University

INSRV launched a project to upgrade and rationalise identity information three years before the Shibboleth project was started. The IDM project was an enabler for the Shibboleth project, and conversely the Shibboleth project gave an additional spur to the IDM project: implementing Shibboleth reinforced the need for clear policies and guidelines for user entitlement to services and resources.

University of Warwick

Warwick has an ongoing project (initiated in early 2006) to rationalise its identity management processes and systems. It is moving towards an architecture of one central directory service and several satellite services.

2.5.7 Access management is implemented using access controls. Access controls often encompass credentials (*eg* username/password combinations) and associated processes (*eg* registration, issuance, authentication, modification). Credentials are issued to users and managed via their identities. For example, a user's entitlements will be revoked when they leave the institution. Access management depends upon identity management.

There are substantial opportunities and resulting benefits for larger institutions to integrate their identity and access management infrastructures.

2.5.8 Identity management supports access management and many of the benefits of access management. Very often identity management identifies and formalises things that are being done or should be done already. There are challenges in effecting effective identity

12 See, for example, the UCISA Top Concerns Survey 2006/2007 and the JISC-funded identity project <http://www.identity-project.org>.

management but institutions are increasingly realising its worth as identity information is crucial to many institutional processes.

2.6 What is the role of licence management?

2.6.1 In order to get users' entitlements right for licensed services, it is essential that licence terms and conditions are fully understood. For many licences, entitlements are based on broad roles such as member of institution, staff, student, *etc*. This will inform the range of attributes required for each user. Other licences will require fine-grained access controls, *eg* a subscription to a resource that is only licensed to one class for one term each year. Service providers must trust that institutions provide accurate identity information.

2.6.2 Access management depends upon effective licence management. Fully understanding licence terms means entitlements are well definable and access controls implemented to support entitlements. Effective licence management also:

- mitigates the risk of contravening licences and missing deadlines to renew;
- facilitates better management reports;
- enables efficiencies when faced with a large and growing collection of resources and services.

2.7 Terminology

2.7.1 The JISC provides a glossary and definitions of the key concepts on its website.[13] This toolkit uses that terminology throughout. Note that:

- A user accesses a "service" even if the service is primarily hosting resources (*eg* email, electronic journals, learning objects); this term is used for any resource or service offered to users that requires access controls.
- "Services within the Federation" are those provided by service providers who are members of the Federation. These include all the resources and services currently protected by Athens, and any new offerings from service providers who have joined the Federation but not previously supported by Athens. Obviously institutions and users must be entitled to use these services even if a member of the Federation. Note that the interoperability provided by the gateway interfaces also allows Athens users to access, if entitled, all services within the Federation.
- "IT Services" and "Library Services" are the terms used for the bodies responsible for provision of such relevant services and support. It is acknowledged that institutions can have other names (*eg* IT Department, University Computing Services) and that the services may or may not be centralised and / or converged.
- Single sign-on (where once logged in all services may be accessed) is distinguished from unified sign-on (where the user must log in to each service separately, but with the same

13 Follow links from the federated access management page at <http://www.jisc.ac.uk/federation>.

credentials at each). The term "simplified sign-on" is used to denote an improvement in the user experience of access controls, perhaps using single or unified sign-on.

- The term "Shibboleth profile" is used for the SAML profile which defines the protocols for the exchange of identity information, whereas "Shibboleth technology" is one implementation of the profile as developed by Internet2.

- An institution will plan and conduct a "project" to "adopt" federated access management. It will then "operate" the federated access management infrastructure.

- Adoption can encompass a mix of technical activities, which depend on the objectives and intended plan, including "development" (*ie* writing code), "implementation" (*ie* installing and configuring software for use) and "deployment" (*ie* rolling out, establishing and running new or revised services).

3 Strategic fit

3.1 Introduction

3.1.1 The first consideration of the toolkit is how potential changes fit with strategic issues and drivers. This "big picture" is important because access management can have a wide scope and significant impact. It is also important to ensure that each institution "does the right thing" and then "does things right". This requires looking at how access management requirements are being met and assessing how federated access management options might fit in with institutional strategy and other activities.

3.1.2 This section asks important strategic questions, and provides guidance, for considering change. It is necessary to have a good understanding of institutional access management requirements to answer these questions. A top-level set of common requirements is provided for information and discussion at Annex B.

3.2 Questions and content

3.2.1 Questions that must be addressed:

- Why do we have to change and does it have to be done now?
  - Are access management requirements currently being met?
  - What internal and external strategic drivers are there for change?
  - What business needs and user requirements are not being currently addressed?
  - How will these needs and requirements change in the future?

- If we must take it forward, how does it fit in with institutional strategy and other activities underway?
  - What does our information strategy say about access management?
  - What does our information strategy say about identity and data management?
  - Is our strategy right?
  - How might any course of action compare to other activities in terms of priorities?
  - What is our and the institution's risk appetite?
  - What is our approach to open-source and community-supported technology?
  - To what extent should identity information be controlled within the institution?

- Who are the decision-makers and are other stakeholders and organisations involved?

- Do we understand the potential and desired scope?
  - How many services should be brought together under a single access management infrastructure?

3.2.2 When writing the business case, the minimum content of this section is:

- a description of the business need and its contribution to overall strategy;
- the objectives of the intended course of action;
- an explanation of why change is needed now;
- the key benefits to be realised and how they will be achieved;
- the key risks;
- the critical success factors and how they will be measured;
- the future operational needs of the institution.

3.2.3 The remainder of this section provides information and guidance on a number of the strategic fit questions, namely:

a) Why do we have to change and does it have to be done now?

b) Are access management requirements currently being met?

c) What internal and external strategic drivers are there for change?

d) Does the change fit with institutional strategy?

e) What is our approach to open-source and community-supported technology?

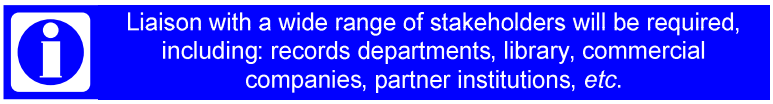
f) To what extent should identity information be controlled within the institution?

g) How many services should be brought together under a single access management infrastructure?

3.3 Why do we have to change and does it have to be done now?

3.3.1 The access management landscape for education and research is undergoing significant change. The Federation has been launched and institutions are invited to join. Athens is moving to a subscription service from August 2008. A decision on the future course of action is required: some change, however minor, is necessary.

3.3.2 It is advantageous to ensure that all key stakeholders are aware of the need to change. It may not be possible to make an informed investment decision without the approval or consent of these stakeholders. There may be autonomous departments or schools with a spread of responsibility for access management. Responsibility for providing and securing certain services may be located away from the centralised services.



3.3.3 Given that the concepts and practice of federated access management are complicated, a degree of educating stakeholders is necessary.

3.3.4 An early lesson from the CM programmes is that IT and library services need to work together on identifying requirements and delivering improvements. Most services within the Federation are bought and managed through Library Services, whereas some federated access management options entail IT Services taking responsibility managing access controls for these services.

3.4 Are access management requirements currently being met?

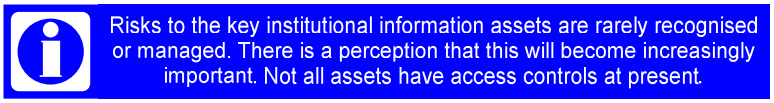
3.4.1 It is necessary to consider what requirements there are for access management. This will entail determining what electronic services are provided and what levels of protection are needed from legal and security viewpoints. The user experience is important. Many

institutions are working towards single sign-on for most services, making the experience as "seamless" as possible for users. Requirements will change in the future, for example as more e-Learning and e-Research services are adopted and used.

Kidderminster College

ICT services has the clear goal that "all resources and services should be accessible using single sign-on and within three clicks". This goal is easy to measure and drives system requirements.

3.4.2 Some requirements might be stronger than others and trade-offs necessary. For example, assurance requirements might be more important than certain usability requirements.



3.4.3 Having thought about requirements it is necessary to consider how well those requirements are broadly being met. For example:

- Where there is extant single sign-on, many commonly used services will meet usability requirements.
- Where there are sensitive systems, complex and audited passwords will meet security requirements.
- Where licensed services are used, particular processes, for example compliance and audit, will enforce certain terms and conditions.

3.4.4 The figure overleaf sets out one exemplar view of existing access controls for user level services, where explicit access controls are not specified for service it is assumed that unique access controls are used (*eg* different usernames and passwords for other licensed resources). To point out that there are a variety of security requirements, some services have been marked as requiring a higher level of assurance.

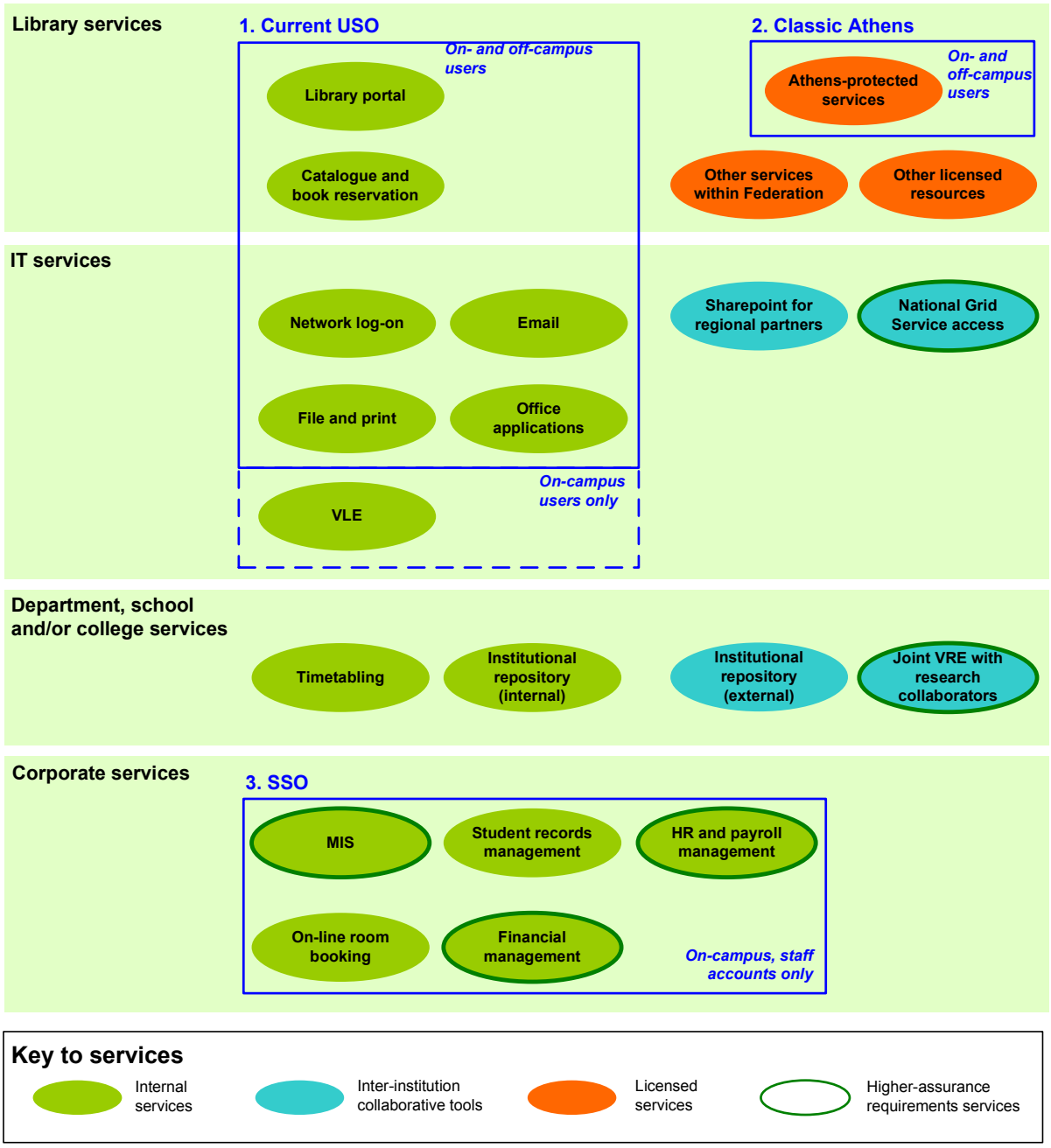


Figure 3-1: exemplar access management environment

3.5 What internal and external strategic drivers are there for change?

3.5.1 It is worth thinking about what strategic drivers the institution and access management faces. A course of action needs to be aligned with the strategic environment and articulating strategic drivers is a useful way of taking account of long-term influences.

3.5.2 There are many strategic drivers common to all institutions; others are more local. Some present opportunities; others are threats. Drivers will cover all areas of the institution, but may be concentrated in areas like governance, business and technical.

Cardiff University

One of the major strategic drivers for replacing the Classic Athens system at Cardiff was the significant administrative and support burden for library staff. Additionally, account creation by IT staff at the start of each new academic year was time-consuming and pressured.

Kidderminster College

The main strategic driver to replace Kidderminster's extant access management systems was the desire to exploit their VLE by making it more accessible and user friendly. This is part of meeting the goal that "all resources and services should be accessible using single sign-on and within three clicks".

University of Surrey

The main strategic driver for replacing the extant Classic Athens system was the significant administrative burden of creating two usernames and passwords for each user. Also, users being required to remember multiple passwords did not provide a satisfactory user experience, and was considered to be a barrier to use of e-Resources.

University of Warwick

The main strategic driver for upgrading the extant Single Sign-On system was the requirement for increased robustness and security of the system against cross-site attack.

3.5.3 Figure 3-2 below illustrates some examples of strategic drivers, with perhaps particularly pressing drivers highlighted in red:

Figure 3-2: exemplar strategic drivers

3.6 Does the change fit with institutional strategy?

3.6.1 Each institution will have extant strategy, policy and plans with which intended changes will fit. It is important to consider the:

- existence and status of the institution's information strategy;
- existence and status of the institution's IT strategy;

Kidderminster College

Kidderminster has adopted a clear strategy for managing its ICT services that includes the principles: strength in depth, centralise services, manage contingencies, document processes and offer interesting work to staff. Opportunities to market expertise are taken and a "collaborative", value for money approach offered; income is used to build up the ICT Services team, thus reinforcing the strategy.

- institutional policies and process for providing and controlling access to electronic information systems (for Management Information Systems (MIS) and for learning and teaching), and whether these strategies, policies and procedures call for a single access management infrastructure across internal and external services;
- whether the institution operates a data-management hierarchy with clearly-defined owners of each element in the process (*eg* joining registering new members, defining rights and entitlements, modifying entitlements, deprovisioning accounts when members leave);
- status and influence of national strategy.

Successful implementations are likely to be driven by institutional strategy and business-critical services.

3.7 What is our approach to open-source and community-supported technology?

3.7.1 The changing access management landscape comes from new concepts, new standards and new technology. The CM programmes were driven by open-source technologies such as Shibboleth. The options outlined later span four broad approaches to procurement and deployment of federated access management technology, namely:

a) commercial tools and support;

b) community tools and commercial support;

c) community tools and support (a mix of community and in-house);

d) institutional tools and (fully in-house) support.

3.7.2 In its purest form, users of open-source technology rely on a development community that is willing to contribute to the codebase and to provide support. Sometimes a sponsoring organisation will fund the development of the technology or provide support, perhaps for a "packaged version" of the technology. There are commercial and academic models for this type of contribution. At the other end of the spectrum, the technology is proprietary and support is bundled in. Institutions also develop and maintain their own technology, particularly when it is considered that no other option meets the requirement. There are many models of development and support. Across all, the concept of open standards should be differentiated from open technology.[14]

3.7.3 Although one of the drivers towards a federated access management landscape has been open-source and community support technology there is an increasing range of commercial technologies available that might be more appropriate. Although it is difficult to generalise the appropriateness of the different models, organisations often have different approaches to open-source and community-supported technology.

3.7.4 Institutions have different risk appetites for deploying new technologies, ranging from innovator, early adopter, majority user through to laggard. This risk appetite and ability to manage risk will inform the approach to new technology, and community tools and support in particular.

3.7.5 It is important to consider whether the approach fits the institution. This covers perceptions of software characteristics, willingness to contribute, support requirements, capability to support, risk appetite, *etc*.

3.8 To what extent should identity information be controlled within the institution?

3.8.1 Institutions hold a range of identity information about users for a variety of purposes. It is typically held on a mixture of systems managed by an array of departments. However, it can be all considered internal to the institution even if not centralised in a single store. Identity information relevant to users' membership of the institution is also held by organisations external to the institution, for example by student loan services, and outsourced payroll services and learning resource providers.

3.8.2 Identity information is increasingly important. Control of identity information is significant from business and legal viewpoints. For example, it is essential that staff and student information is kept accurate, alumni contact information exploited intelligently, the use and release of identity information covered by the Data Protection Act, *etc*.

3.8.3 Control of identity information encompasses various aspects including ultimate responsibility, delegated day-to-day control, ability to administer and maintain, auditability, *etc*. The key concept of federated access management is an institution will manage more of its users' identity information, passing agreed information to service providers to authorise access.

3.8.4 Sub-section 2.5, on identity management, demonstrated the importance of using identity information effectively. External control of identity information is a strategic-level issue and it is necessary to decide when and how external control is part of institutional strategy. For

---

[14] There is a widespread and beneficial trend towards open standards: open standards enable interoperability and reduce switching costs from one solution to another, preventing lock-in.

example, external control might be permitted where beneficial, or identity information may be considered a strategic asset to be managed in-house wherever possible.

3.8.5 The strategic choices outlined later span a range of levels of institutional control of identity information: including full institutional control and transferring certain information to a third-party as part of an outsourcing contract.).

3.9 How many services should be brought together under a single access management infrastructure?

3.9.1 Information and communications technology is increasingly important within the normal course of business. The range of services is growing and covers most aspects of and processes within institutional life. Understanding access management requirements entails identifying all such services that require access controls.

3.9.2 Many institutions will already have unified or single sign-on that federated access management can utilise. This may meet many access management requirements: do users have seamless access to all services to which they are entitled? Other institutions may be looking to deploy improved sign-on technology at the same time as federated access management.

3.9.3 The strategic question is which services could and should be provided through a single access management infrastructure. Assuming establishing a single federated access management infrastructure is conceivable, the questions to consider are:

- Which internal services should be brought together with simplified sign-on?
- Should licensed services be included?
- Is an access management infrastructure required for inter-institutional collaboration?

3.9.4 These categories of service, or a more detailed analysis, determine the intended scope of a single federated access management infrastructure. The options outlined later range from a small and restricted scope through to establishing a single federated access management infrastructure that is a flexible and extensible enough to expand in the future.

3.9.5 Not all services offer, or can easily support, federated access management. Some are not web-based, some have built-in access controls and some do not yet support federated access management. The services within the Federation do support federated access management as do many others.[15] The CM programmes led to a number of services being configured for support: some are now easily configurable, others remain challenging. It is necessary to consider whether the services, particularly internal services, can support federated access management.

---

15 See the JISC's federated access management website for information on products and services that support federated access management, *eg* VLEs at <http://www.jisc.ac.uk/news/stories/2007/02/news_vles.aspx>.

3.9.6 There are significant benefits of a single access management infrastructure, but this is obviously a much greater, and likely riskier, undertaking: a wide or all encompassing scope is likely to be a strategic-level decision.

Internal services

3.9.7 An important consideration is how centralised / distributed provision of information, IT and library services is within the institution. Strongly autonomous departments and libraries, and limited centralised services, may preclude a wide scope. Consolidated IT infrastructures with a broad range of infrastructure and services to all users may make it easy to have a wide scope.

Licensed services

3.9.8 The move to a subscription service for Athens has a relatively narrow scope (*ie* licensed services currently protected by Athens) in terms of all the services that any institution provides and uses. The Federation is expected to encourage new service providers to join, leading to more services within the Federation.

Kidderminster College
Network services, the portal, VLE, repository and Athens-protected resources were in scope. The library will continue to support a range of access controls for resources that do not support use of federated access management.

Inter-institutional collaboration

3.9.9 Increasing inter-institutional collaboration may be one driver for a single access management infrastructure, for example for sharing, in a controlled manner, modules within a VLE, learning objects from a repository or collaborative tools for research. Some institutions may not find this a key driver. It is necessary to consider what common partners are planning: collaborative infrastructure is more beneficial the more extensive it is.

Exceptions

3.9.10 The minimum scope is those services within the Federation. The broadest scope will include many of the previously identified services. However, it is unlikely that all services will be in scope, for example:

- Existing access controls may not be under institutional control: they might be for third-party resources or for legacy systems with built in access controls.
- Schools and departments may autonomously run services that do not fit, or can not easily be brought, into scope.
- Security or technical concerns may rule out bringing access controls for administrator accounts onto a single access management infrastructure.

- Certain services, such as those provided by niche publishers, may use their own access controls (*eg* issuing user or group usernames and passwords) and may not be part of the emerging federated access management infrastructure.

Exemplar

3.9.11 One possible intended scope is illustrated below. Note that it not a single infrastructure: corporate services for staff use separate access controls, and certain licensed and Grid services also use other controls. It can be compared to the current environment example above, in Figure 3-1.

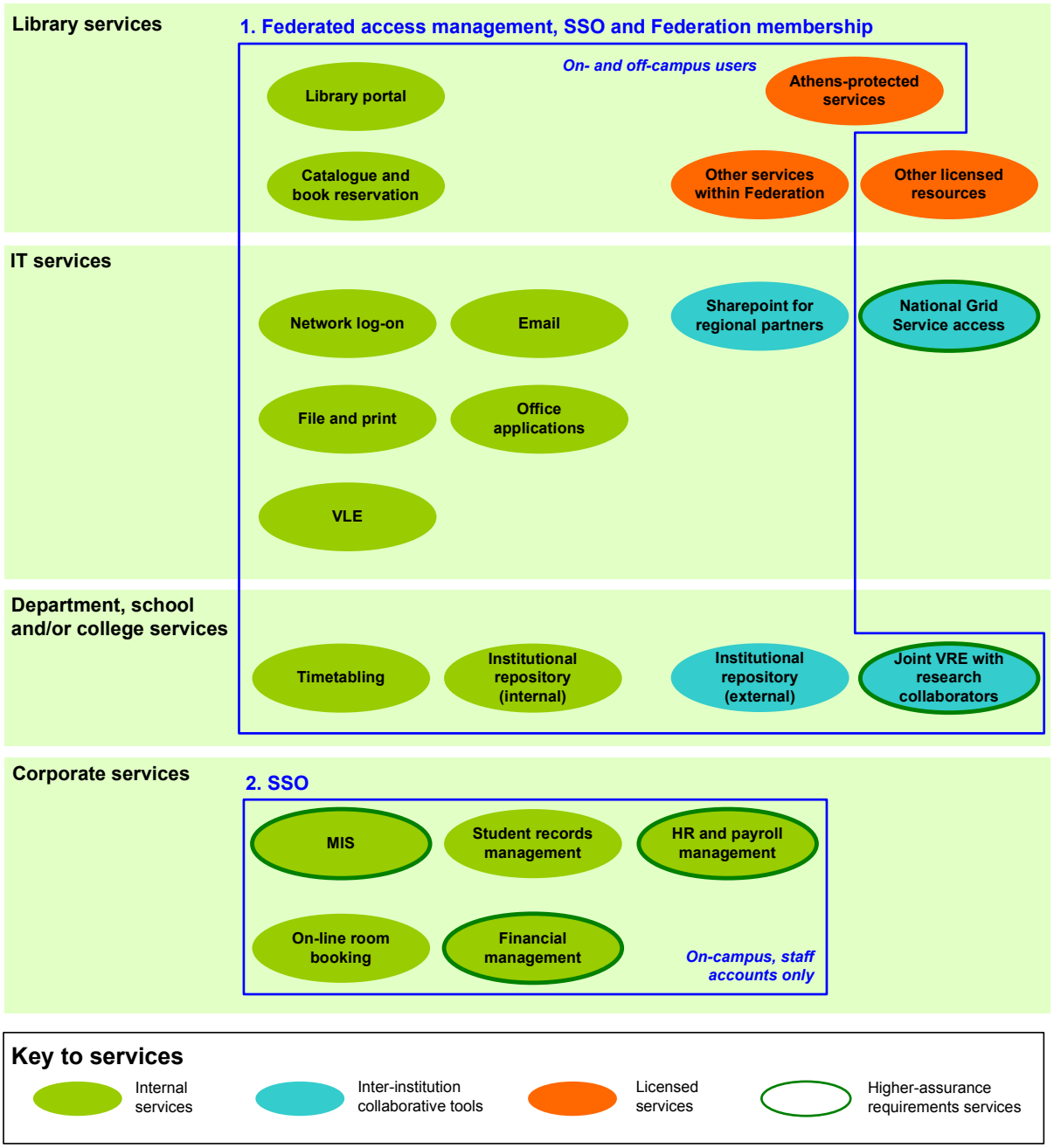


Figure 3-3: exemplar scope of federated access management infrastructure

4 Options appraisal

4.1 Introduction

4.1.1 Understanding the options available, and justifying which to choose, is important in decision-making. One approach to doing this, considered good practice, is an options appraisal.[16] It provides an objective and evidence-based way of evaluating competing alternatives. Completing it fairly and accurately often requires asking questions and gathering information for any gaps. Completing an options appraisal will usually lead to a preferred option (see sub-section 4.3).

4.1.2 Obviously choices will be made throughout the change, from overall direction through to decisions on detailed implementation options. This section is concerned with overall direction of an access management strategy. Specific decisions will "flow" from the initial choice of top-level option and consideration of institutional circumstance. The range of choices will vary, and will undoubtedly change as the access management landscape progresses.

4.1.3 This section addresses the "economic case" by examining a range of access management strategies. Completing an appraisal assesses the options (sub-section 4.4) against their benefits (sub-section 4.5), costs (sub-section 4.6), risks (sub-section 4.7) and timescales. The preferred option offers the optimum mix.

4.2 Questions and content

4.2.1 Questions that must be addressed:

- What options are there?
- Is the range of options under consideration sufficiently broad?
- Have innovative options and/or collaboration with others been considered? (If not, why not?)
- What are the option criteria?
  - Are all benefits, costs, risks and timescales covered?
  - Are all business needs, requirements and characteristics covered?
  - Would other stakeholders agree with the option criteria?
  - Are criteria weightings necessary?
- What benefits, costs, risks and timescales are associated with each option?
- What option has the optimum balance of cost, benefit and risk?
  - What trade-offs need to be made? (*eg* foregoing some of the benefits to keep costs within budget)

4.2.2 When writing the business case, the minimum content of this section is:

- a cost, benefit and risk analysis of at least three options for meeting the business need;
- the identification of preferred option, with any trade-offs.

---

16 See, for instance, *Investment decision making*, *A guide to good practice*, HEFCE, April 2003.

4.3 How to decide using an options appraisal

4.3.1 An options appraisal is a means of comparing different options.[17] The basic process encompasses the following steps:

a) identifying and defining relevant options and assessment criteria;

b) assessing each option against each criterion;

c) aggregating marks to yield the preferred option.

4.3.2 Often the criteria will not be quantifiable and not easily comparable. Techniques such as rankings or shadow values (*eg* 1 through 5) to compare options may be used.

4.3.3 The aim of this options appraisal is to assess the optimum mix of benefits, costs, risks, timescales and other factors in light of the strategic fit considered in the Section 3. This is then assessed for affordability in Section 5.

4.3.4 A (simple) exemplar options appraisal is set out in Figure 4-1 below:

		Option 1	Option 2	…	Option n
Benefits	(most scores highest)	4	2	…	3
Cost	(least scores highest)	5	1	…	3
Risks	(least scores highest)	3	2	…	4
Other assessment criteria	(best scores highest)	4	4	…	5
Total	(highest is best)	16	9	…	15
Preferred option		✓			

Figure 4-1: exemplar options appraisal

4.3.5 Options appraisals are often hard to conduct, for example requiring information that is not available or forcing excessive deliberation. Nevertheless, they are a useful tool for comparing and analysing options fairly and objectively.

4.4 What options are there?

4.4.1 There are a number of decisions that need to be made, covering as a minimum strategy, Federation membership and deployment choices. A number of options that encompass these aspects can be listed for the options appraisal. This sub-section discusses the various decisions and illustrates the process with a set of exemplar options.

---

17 See, for instance, JISC infoNet (<http://www.jiscinfonet.ac.uk/infokits/learning-space-design/implementation/forward/options-appraisal>)
or the Treasury's Greenbook (<http://greenbook.treasury.gov.uk>) for more information.

Strategic choices

4.4.2 Each institution already has a strategy and approach for meeting their access management requirements. It is necessary to decide if and to what extent federated access management should be adopted as a strategy. The choices are:

a) **do not adopt federated access management**: no internal changes are assessed necessary. The current range of access controls is maintained.

b) **deploy a limited federated access management solution**: a limited deployment is made, for example to get access to services within the Federation. A similar range of access controls is maintained with limited simplification. This is likely to need a project to deploy and some ongoing effort.

c) **deploy a single federated access management infrastructure**: moving towards unified access management, for example using federated access management to enable simplified sign-on to all services chosen to be in scope. This is likely to require to a substantive deployment and business change project, or number of projects, and then ongoing operation of "mission critical" infrastructure.

UK Federation choices

4.4.3 The UK Federation for Education and Research has been launched and institutions have been invited to join. Particularly from August 2008 this choice will have a significant impact on how services that are currently protected by Athens are accessed. The choices are:

a) **do not join the Federation**: this choice will make it more difficult to access licensed resources that are within the Federation and currently protected by Athens after July 2008. In reality, this choice might mean stopping using these services, organising alternative access controls for these services or making a rushed alternative choice; all of which will require substantial effort and with significant downsides. This choice will be unpalatable to many institutions since staff and students may not be able to access the full range of resources and services that are currently in use.

b) **join the Federation as an identity provider**: this choice involves adopting federated access management and being able to supply attributes to services within the Federation in order to get access. It is necessary to sign-up to the Federation and provide certain metadata with this option. It is important to understand the terms and conditions of the Federation and ensure they can be and are met.

c) **join the Federation through an outsourced identity provider**: this choice means that another entity handles the identity provision for services within the Federation; the institution will need to support this entity as necessary, for example by supplying and maintaining identity information. It is necessary to sign-up to the Federation and provide certain metadata with this option. Athens, encompassing Athens Classic and AthensDA, is transitioning to the Federation as an outsourced identity provider under the name OpenAthens. It is envisaged that other suppliers will emerge to provide further choice. Even under outsourced identity provision, there are a range of sub-options. For example, AthensDA permits institutions to keep control of identity information and use existing authentication mechanisms (perhaps with single or unified sign-on), leading to many of the benefits as in the full federated model, only the entitlement policy is outsourced.

Combined strategic and Federation choices

4.4.4 The strategic and Federation choices are interdependent: the ways in which they can combine are (darker shades indicate more unlikely combinations):

	Do not join the Federation	**Join the Federation as an identity provider**	**Join the Federation through an outsourced identity provider**
Do not adopt federated access management	Only sensible if alternative access controls can be organised or there is no need for those services	Not possible: technical and policy requirements not met	Certainly a viable option and maybe the best of the "do not adopt" choices
Deploy a limited federated access management solution	Unlikely to be a sensible option: any deployment is likely to be used to join the Federation as an identity provider and retain access to services	Unlikely to be a strategic decision but may meet immediate requirement. May be transition to a single infrastructure	May be transitional to joining the Federation as an identity provider, or part of a mixed strategy
Deploy a single federated access management infrastructure	Unlikely to be a sensible option: any deployment is likely to be used to join the Federation as an identity provider and retain access to services	Certainly a viable option and probably the end outcome for some institutions	May be transitional to joining the Federation as an identity provider

Figure 4-2: combined strategic and Federation choices

Deployment choices

4.4.5 If deploying federated access management, it is necessary to choose a top-level approach to the technology. Experience has shown that this choice can influence or determine the preferred option. There is an increasing array of technologies and services to choose from, though these can be usefully categorised by source of technology and type of support, offering the choices:

a) using community tools and community support;

b) using community tools and commercial support;

c) using commercial tools and commercial support;

d) using tools developed in-house and internally supported.

University of Warwick

The E-lab developed a system that implemented the Shibboleth profile for federated access management of its web applications. This software is maintained in-house though it remains possible to switch to community supported tools (eg Shibboleth technology) if desired.

Other choices

4.4.6 Other institution-specific issues can help identify useful options. For example, institutional mergers / consolidation, other organisational changes, governance changes, strategic reviews, legacy system changes, *etc*. These may give rise to new or modified options. Any option that seems a reasonable possibility should be considered.

Exemplar options

4.4.7 The above choices can be combined to form options for the appraisal, for example:

a) retain current access controls, join the Federation through an outsourced identity provider and "wait and see" with to regards federated access management, reviewing decision in two years;

b) retain current access controls, join the Federation through an outsourced identity provider and "wait until the conditions are right" (*eg* deployment of directory services, initiation of identity management project or availability of appropriate commercial solutions) with regards federated access management;

c) deploy a limited federated access management solution using community tools and support, join the Federation as an identity provider and start moving to a single infrastructure;

d) deploy a limited federated access management solution using community tools and commercial support, join the Federation as an identity provider and start moving to a single infrastructure;

e) deploy a single federated access management infrastructure using a commercial partnership and join the Federation as an identity provider;

f) procure and deploy a single identity and access management infrastructure and join the Federation as an identity provider.

4.4.8 At some point it is worth considering what sub-options are available, for example what technology to use, or whether to go for a "big bang" deployment instead of a phased deployment over two or more years. Sometimes there is merit in culling some options with a "first pass" options appraisal before looking at remaining options in more detail (*eg* for technical feasibility) with a "second pass". In general, it is important to get the "big picture" right even if the details have significance.

4.5 What benefits might there be?

4.5.1 A range of benefits are available depending on the option chosen, planning and exploitation and the success of the project. Not all benefits can be quantified in financial terms; some are more strategic or cultural. It is important to consider what benefits are desired and which benefits can be realised, and for who, for each of the options under consideration.

4.5.2 This sub-section introduces an exemplar set of benefits to institutions from federated access management and discusses how they might be realised. They are introduced in two stages: firstly "basic benefits" and then "wider benefits" from the context of the Federation and the JISC's initiative. "Benefits maps" are used to show the path to realising benefits, illustrating the elements required to realise each benefit:

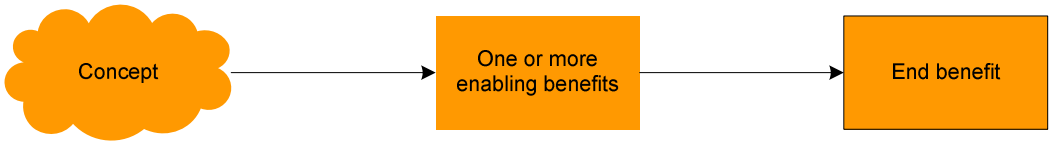


Figure 4-3: a benefits map

Basic benefits

4.5.3 In its most basic form, there are two underlying concepts to federated access management:

a) **Authentication and authorisation separated**: the institution is responsible for authentication and can use an existing authentication mechanism. The service provider is responsible for making access decisions, based on information provided by the institution.

b) **Use of attributes**: attributes (*ie* pieces of identity information in a defined format) are supplied by the institution to the service provider in response to requests. The service provider uses this information to make authorisation decisions. For example, the service provider might ask for the name of the institution and department of the user trying to access a service; if the response matches their list of licensees then access is granted (or declined if not).

4.5.4 Figure 4-4 below shows the basic benefits map:

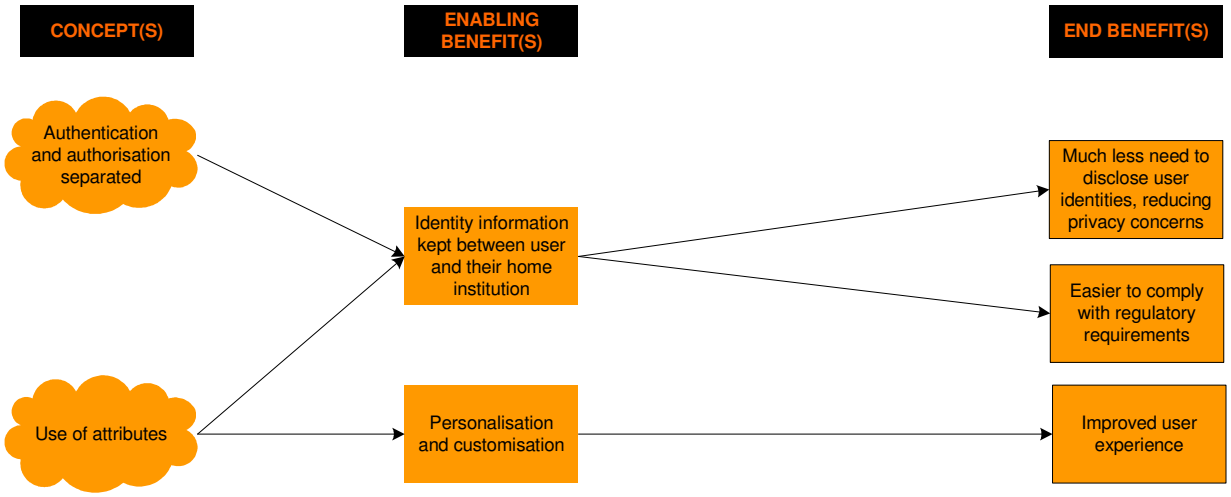


Figure 4-4: exemplar, basic benefits map

4.5.5 The end benefits are:

- **Much less need to disclose user identities, reducing privacy concerns**: users benefit because separation of authentication and authorisation and the use of attributes means more identity information can be kept between users and their institution. For example, users may be able to access a service without disclosing their name and email address to the service provider. The release of identity information can be controlled through agreement with users and service providers when properly implemented. Although unquantifiable, many users, if aware, may find this reduced disclosure reassuring.

- **Easier to comply with regulatory requirements**: a similar benefit accrues to institutions: the administrative overhead and problem of compliance with regulation affecting disclosure or transfer of identity information reduces. Less identity information can be inadvertently, or maliciously, disclosed if less is shared.

- **Improved user experience**: the use of attributes can enable personalisation (*ie* user-selected modifications) and customisation (*ie* administratively-determined per-user capabilities) by the service provider. When appropriate and well implemented, personalisation and customisation can "add value" to new and existing services.

Wider benefits

4.5.6 The term federated access management is used here within the context of institutional strategy, the Federation and the JISC's initiative. This wider view encompasses extra concepts and enables further benefits. The additional concepts include:

- **Fine-grained access controls**: access decisions can be made specific and individual to the circumstances. For example, instead of granting an institution universal access to a publisher's set of services, specific year or subject groups can be given access to a sub-set of services. Fine-grained access controls provide this capability, though it is still

necessary to agree and manage the entitlement policy, which, being more complex, is a greater overhead.

University of Surrey

Surrey has an increasing number of user groups that are "special cases", for example foundation degrees for international students, an overseas institute and a local agency who can award degrees to students who are not members of the University. Fine-grained access controls would permit library services to decide whether to offer some of its e-Resources to these groups.

- **Unified access management**: a common means of using complete, consistent, timely and accurate processes for permitting or denying access to protected services. This comprises an entitlement policy that spans all users and all services; for each user-combination there are clear access rights, with any supporting requirements, *eg* a level of assurance. Unified access management can be realised in many ways and will involve a single access management infrastructure of some sort.

- **Unified identity management**: effective identity management and a common means of accessing identity information. This can be implemented in a range of ways from complete centralisation (*eg* central processes and a single system); through highly distributed approach with a lightweight overarching framework (*eg* meta-services to aggregate sources of identity information). Users themselves can be included with the principle of self-service where users themselves directly manage their identity information (*eg* maintaining contact details or self-service password resets), realising benefits such as more accurate and timely information and reduced administrative overheads. Identity information is propagated or synchronised as appropriate, with a degree of coupling. Regardless of how implemented, identity information is accessed through common means.

- **National and international support and uptake**: the UK's Federation has counterparts in an increasing number of other countries. SAML, the Shibboleth profile and technologies such as Shibboleth are often the foundation.[18] SAML is a standard not specific to the education and research sectors and has seen uptake for a range of applications.

- **Open standards**: SAML is an openly published technical standard. Similarly the Shibboleth profile is published and developers can implement it if they wish. In this context, open standards enable greater consistency across the whole of education and research, though offer many ancillary benefits such as reduced lock-in to proprietary systems and vendors.

4.5.7 Unified identity management supports unified access management. Together they are potent combination. Although both are idealised and their attainment faces many challenges, there is increasing realisation in the public and private sectors that the benefits can be considerable.

4.5.8 Figure 4-5 overleaf shows the full, exemplar benefits map. Because identity management is different to, but integral to, access management the colour purple indicates which benefits require unified identity management.

---

18 *Federated access management: international aspects*, CC253D018-0.2, March 2007.

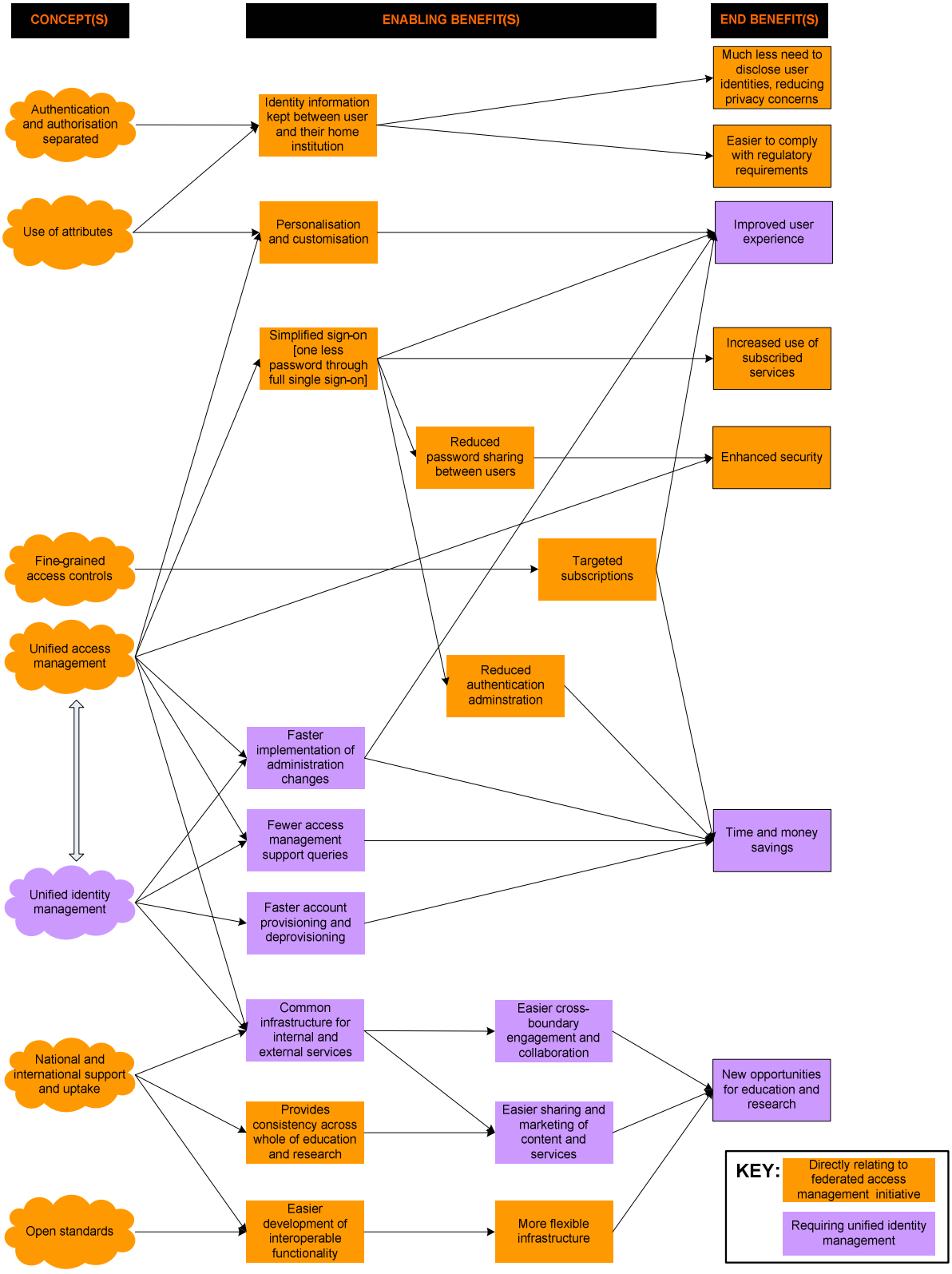


Figure 4-5: exemplar, wider benefits map

4.5.9 Additional end benefits include:

- **Increased use of subscribed services**: enabling simplified sign-on means services are easier to access. Having to remember an extra and unique username / password poses a "barrier" to access (for good security reasons) and use (perhaps more unreasonably). Where the same password can be used across a number of services but must be entered each time (*ie* unified sign-on) enabling simplified sign-on makes the process more "seamless". Many believe that simplified sign-on services are experimented with and used more. Where subscription services are expensive this may be an important benefit. Obviously, productive and effective use of the services is not assured but greater use is normally seen as beneficial.

- **Enhanced security**: security for users, the institution and service providers benefits in two main ways. Firstly, simplified sign-on may lead to reduced password sharing: a user is much less inclined to reveal a password that enables access to personally important email than a set of learning resources. Secondly, rationalising access controls presents a smaller attack surface and means that the remaining access controls can be tightened as required (the danger is that security reduces to the weakest of all). Clearly overall "security" is still dependent on a range of physical, personnel and process factors.[19]

It is expected that implementing single sign-on will cut down password proliferation but increase the risk for any single password loss. Therefore, passwords will continue to be a weak link.

University of Warwick

A significant benefit of implementing Shibboleth technology at Warwick is increased security. Security is a particular concern at Warwick due to the large number of internal web services that allow users to publish their own material. Furthermore, users have more inhibitions about sharing their local Warwick password than their Athens password.

- **Improved user experience**: users benefit from better middleware in various additional ways, including:

  - Simplified sign-on reduces the "mental overhead" of remembering usernames and passwords and entering them multiple times.[20]

Users may use passwords as part of personal, unofficial access controls. Coarse-grained authentication mechanisms (*eg* a single password) may lead to user inconvenience.

  - Unified access and identity management can lead to more responsive and correct services to users as administrative changes are reflected better in what the user can and cannot access.

19 See, for example, the UCISA Information Security Toolkit, <http://www.ucisa.ac.uk/ist>.

20 Some evidence of this is given within *Highlights and Conclusions from Trialling Shibboleth* from the WALRUS project, <www.wakefield.ac.uk/projects/walrus>.

Cardiff University

One of the major benefits that federated access management has brought to Cardiff University is an enhanced user experience. Users are now only issued with a local Cardiff username and password (which has also reduced the administrative burden), and Athens protected resources are now part of their unified sign-on system.

A large number of existing users migrated ahead of schedule, without publicity, to realise the benefits of the enhanced user experience introduced for all new intake.

Kidderminster College

Kidderminster now has a single sign-on system for access to the network and web resources (including the VLE), improving the user experience. A significant benefit of federated access management for Kidderminster is that external users can now access the Kidderminster VLE. This is much more convenient for distance learners who are based externally to Kidderminster for the majority of the time.

- Fine-grained access controls offer the possibility of restricting the user group for a particular service. This capability is beneficial, for instance, where a subscription is unaffordable if it had to be universally licensed, but could be offered to a specific group (*eg* a single course or type of user). Such targeted subscriptions are only possible where access controls can enforce licence agreements. Finer-grained access controls have an associated overhead.

- **Time and money savings**: improvements in efficiency, which can be translated into time and/or money savings, come from a variety of sources:

  - Targeted subscriptions can be used in place of universal licences, saving the institution money.

  - Simplified sign-on means fewer credentials need to be generated, issued, managed, changed when forgotten and retired. This can be a significant benefit for institutions with previously many types of credential and a high change rate.

Cardiff University

A significant benefit for Cardiff has been a faster turnaround of course changes for students. Previously getting access to course material on the VLE following a change of course took several weeks due to the administrative process, particularly at the start of the academic year when there are many changes. This was far from ideal. Now entitlement policy is changed straightaway and students can immediately get access to the right course materials.

University of Surrey

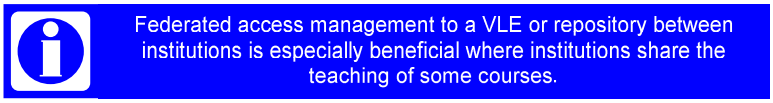
In addition to enhancing the user experience and reducing administration overheads, adopting AthensDA has forced Surrey to upgrade their identity management processes, and responsibility for authentication is held by the institution. This is considered to be one step closer to being ready to adopt federated access management.

An additional benefit is that AthensDA is supported externally by Eduserv. This suits Surrey's lean staffing structure and limited experience with open source technology.

  - Unified access and identity management provide a number of opportunities for efficiency improvements, for example: more accurate implementation of administrative changes saves staff having to check entitlements and the costs of later correction; fewer access management support queries (*eg* checking and changing user entitlements); and, automated account provisioning and deprovisioning mean much less effort is required to prepare for new users, and that previous users will no longer be allocated accounts and related licences. Accurate user records leads to better management information and potential savings. These savings can be considerable.

- **New opportunities for education and research**: it is hoped that properly effecting unified access and identity management based on open and global standards will lead to significant opportunities and benefits. A single access management infrastructure within an institution is an enabler for exploiting opportunities. A single access management infrastructure across education and research makes cross-boundary collaboration easier and can facilitate sharing and marketing of content and services. Use of open standards makes new development work easier and leads to a more flexible infrastructure. Much of the benefit of the infrastructure could be as yet unrealised applications. Examples of emerging opportunities include:

  - facilitating new courses by allowing aggregation of distance learners to use a VLE, or enabling a college to offer foundation degrees by using modules or content from universities, or marketing courses to businesses;



  - assisting easier access to Grid resources and services;

  - establishing a regional federation to encourage and facilitate collaboration;

Kidderminster College

Resources can now be securely shared between institutions, opening up possibilities for inter-institutional access to resources; some courses are already shared with regional partners.

  - facilitating international collaboration through sharing of resources and services.

Kidderminster College

Working with open source software has proved stimulating to the development team, has helped with staff retention and marketing its expertise has allowed expansion of the department.

4.6 What are the potential costs?

4.6.1 The anticipated costs of each option are obviously important considerations. Experience has shown that the cost of adopting federated access management will vary widely between institutions: the combination of different legacy systems, scopes, skill sets, approaches to deployment, *etc* make it clear why this is so. This sub-section sets out some of the issues to consider, including a process to estimate costs and some of the costs from early experiences of federated access management.

4.6.2 Many costs will be borne from existing budgets and overheads, and may not show up as explicit costs. This means including indirect costs (*eg* staff training and ongoing administrative support) as well as direct costs (*eg* cost of hardware purchase, subscription costs).

4.6.3 Assessing through-life cost provide a realistic basis on which to compare options. This means including upfront costs (*eg* hardware costs, subscription negotiation costs) as well as ongoing costs (*eg* hardware replacement costs, annual subscription fees) over the entire lifetime. Methodologies such as discounting and including depreciation can be used if required.

4.6.4 Although harder to estimate, identifying direct and indirect costs and using through-life costs (or Total Cost of Ownership (TCO)) will lead to better decision-making and is considered best practice.

4.6.5 It is possible to determine the cost differences between options, rather than absolute costs. Where time and money savings are likely this approach might be easier, and more illustrative.

4.6.6 It is worth noting that an estimated cost profile over the duration of the project and operation is needed to assess affordability (Section 5).

4.6.7 A typical investment requires high upfront costs in return for lower operating costs. This scenario is likely with a full adoption of federated access management versus using an outsourced identity provider, though the benefits accrued will also vary; choosing an option need not just be a financial argument. Where comparing two options with this scenario it is important to consider the robustness of the "pay-back period", *ie* if shortened or extended does the comparative advantage still hold?

4.6.8 Some costs will be clear whereas others will have significant uncertainty. For example, an outsourced identity provider may provide a clear set of charges upon for which through-life cost can be easily estimated; significant projects of business change might be difficult to estimate in advance. Uncertainty can be explicitly represented as risks.

Cost categories

4.6.9 A helpful way of estimating through-life costs is to use compare options objectively across a number of categories. Exemplar categories, for a project and subsequent operation as an instantiation of an option, are as follows:

- **Upfront project costs**:
  - **Establishing prerequisites**: some options need prerequisites that may require effort or procuring if not already present. For example, deploying federated access management requires an attribute store (*eg* directory services), effective identity management processes and a clearly defined entitlement policy (see Section 7 for details).
  - **Development effort**: development staff may be needed to implement or integrate systems. Often internal staff can be used but sometimes external expertise may be required.
  - **Direct costs**: such costs are necessary for some options and include hardware, software, project management, *etc*.
  - **User training**: where change will occur there will be an upfront training effort required, for example technical skills training, training librarians, training students and staff, revision of support materials, *etc*.
- **Ongoing operation costs**:
  - **Membership and subscription fees**: there are no fees at present for the Federation. An outsourced identity provider is likely to use a subscription model: subscription fees for OpenAthens for AY 2008/09 are already available and are calculated according to JISC Collections banding.
  - **Support costs**: these may be direct (*eg* commercial support contracts) or indirect (*eg* in-house support and extra administrators) costs needed to ensure that systems and services are maintained appropriately (*eg* managing upgrades).
  - **Administrative costs**: all access management requires administrative effort such as user registration, issuing credentials, password administration, *etc*. This cost is often substantial.
  - **Hardware replacement**: all hardware needs rolling replacement.
  - **Audit and compliance**: access management requires audit and compliance checking (*eg* regulatory and policy compliance, user misuse). Responsibility for this needs to be ascertained (*eg* it may be part of an outsourced identity provider service) and costs estimated.
- **Opportunity cost**: this considers what is being given up for the option. For example, what other projects or initiatives could be undertaken if the budget or staff allocated required for the option could be freed up?

Experience of costs

4.6.10 Institutions involved with the CM programmes, and others, have some experience with the costs of adopting federated access management. The following figures are for indicative purposes only:

- Internet2 full enterprise directory services example (an attribute store is a prerequisite for federated access management): £220k capital, £150k recurrent;[21]
- Limited technical adoption of federated access management (assuming prerequisites such as those set out in Section 7): £5k;
- Kidderminster College's commercial federated access management offering for other institutions: from £1.5k per deployment, £0.5k annual support costs;
- Early Adopters from the CM programmes (with varying objectives and scopes): £50k.

Cardiff University

Cardiff received £50,000 from the JISC as an Early Adopter of Shibboleth technology and further funding was provided out of the INSRV budget. The total project budget is estimated to be £75-100k.

Additionally, prior to implementing Shibboleth, Cardiff had invested in excess of £1M in upgrading their IDM.

Kidderminster College

Building on its experience of implementing federated access management in-house, Kidderminster College now provides a commercial service to implement and support Shibboleth IdPs and SPs to other institutions. Direct charges are from £1.5k per deployment with £0.5k annual support costs. Kidderminster's experiences indicate that the following activities, and associated internal effort (estimated), are necessary:

- **internal review**: audit of set-up, file store, security *etc*;
- **active directory implementation**: training of in-house staff (5 days); audit (3 days with some assistance); implementation (internally 20-30 days over 6 months, or use external specialists);
- **firewall configuration**: 1 day;
- **setting up attribute store**: 2 days with some assistance.

4.7 What risks need managing?

4.7.1 Each option comes with a number of risks. Some will be top-level and easily identifiable from the option; others are identifiable at a technical or operational level. Each option needs to be risk assessed and top-level risks compared to the institutional and stakeholder risk appetite. For example, the organisation as a whole may be averse to risky, large-scale IT project failures; this will make any such option less appealing.

21 See *Middleware Business Case: Alpha University*, A sample middleware business case, Internet2, October 2001. Approximate breakdown: £37k capital and £4k operating hardware costs; £33k capital and £9k operating software costs; £150k capital and £137k operating staff salaries. Operating costs start in the second year.

4.7.2 Exemplar general and access management risks include:

- using immature technology and policy leads to continual changes and ongoing development effort or additional support effort;
- the risks of project overspend, delay, reduced quality or scope, or project failure, perhaps caused by problems with scale, complexity or uncertainty of project or by failure to address prerequisites;
- establishing a critical service without the means to support and sustain it resulting in operational impacts (*eg* outages, user frustration) in the future;
- access violations or security attacks resulting in financial or legal impacts, loss of trust between institution and service providers or overly restrictive policies on users;
- failure to realise expected benefits: such as publishers offering targeted subscriptions;
- changing environment, such as changing requirements, legislation or regulations, annuls or alters investment;
- faster than expected obsolescence of standards and technology resulting in legacy expense;
- advantages or benefits (*eg* kudos, technical leadership) lost by selecting another option.

University of Surrey

Surrey conducted a formal options appraisal and decided to implement AthensDA in preference to Shibboleth technology. This was primarily because Surrey did not want to be on the leading edge with a production service, and it was imperative that the service was robust: implementations of Shibboleth technology had largely been confined to pilots.

4.7.3 Significant risks can be mitigated. For example a pilot project might investigate business change and potential benefits, and a technical demonstrator might lower technical risk. Understanding whether there is a contingency option (*eg* a fallback to previous access controls) or a contingency budget is helpful.

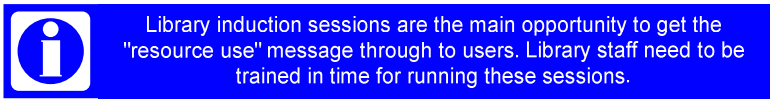
4.8 Additional considerations

4.8.1 In addition to benefits, costs and risks associated with access management, other considerations, as with any project, are often needed, particularly with options that are more detailed. Exemplar considerations, which may included as additional benefits, costs, risks or assessment criteria, include:

- **Alignment with institutional strategy**: does each option match the longer-term direction of the institution, for example fitting with strategic drivers and preferences for control of identity information, scope of access management infrastructure and commercial or community models for tools and support?

- **Meeting business needs and user requirements**: does the option enable the institution to meet better its access management and other requirements? Are all types of requirement considered? For example institutional security policy and licence requirements: will the option permit user auditability?

- **Timescales**: this considers the fit between option and institutional and national timescales. For example, can the option align with the academic year? When can change take place and when can it not? Are there dependencies from other projects? Will the institution have a means of accessing services currently protected by Athens in August 2008? The Early Adopters from the CM programmes generally found it took, in the order of, six months to get the technical side of federated access management sorted: this indicates that proper advance planning is necessary.



- **Scalability, adaptability, agility and extensibility**: these consider the robustness of the option and the impact of future changes: can the option cope with technical, policy, scope, process or other changes? There are often substantial benefits from investing in future flexibility. Conversely there are risks from only considering today's requirements.

University of Warwick

Warwick has positioned itself so that it can join the UK Federation and configure to use full federated access management for accessing third-party resources and inter-institutional sharing when required.

- **Reliability and resilience**: this questions whether the option leads to appropriately dependable services or solutions. A key concept of federated access management is that institutions take responsibility for authentication, therefore the authentication mechanism is likely to become critical. For example, how "mission critical" is access management for the services in scope? Is there a single point of failure? What happens if systems fail at night or at weekends? Can a "mission critical" access management infrastructure be adequately supported?

Cardiff University

Cardiff's single federated access management infrastructure is considered "mission critical": two Shibboleth IdP servers are load balanced and supported by a virtual server. This architecture has been extensively load tested and meets INSRV policy of two servers "up" even during software upgrades and maintenance.

University of Warwick

The E-lab is proud of its achievements in providing a range of high-availability and innovative web services. In moving to single sign-on it has established a "mission critical" service that is managed appropriately, including through rigorous compliance testing and formal configuration management.

4.9 Summary of the options appraisal

4.9.1 This section has:

a) outlined a way to decide, objectively and fair, between different options using an options appraisal (sub-section 4.3);

b) detailed key choices, and resulting options, that must be considered (sub-section 4.4);

c) set out the specific benefits from federated access management (sub-section 4.5);

d) provided a framework for calculating potential costs, together with some example cost figures from institutional experiences (sub-section 4.6);

e) listed a number of general, and access management specific, risks that need to be managed during any resulting project (sub-section 4.7);

f) discussed some further considerations, including additional assessment criteria, and ancillary benefits, costs and risks, in conducting the options appraisal (sub-section 4.8).

4.9.2 The steps in an options appraisal are shown, together with the exemplars used in this section, in Figure 4-6 overleaf.

4.9.3 The options appraisal is an important tool in the decision-making process: used properly it can provide objectivity, obtain buy-in from stakeholders and ensure accountability.

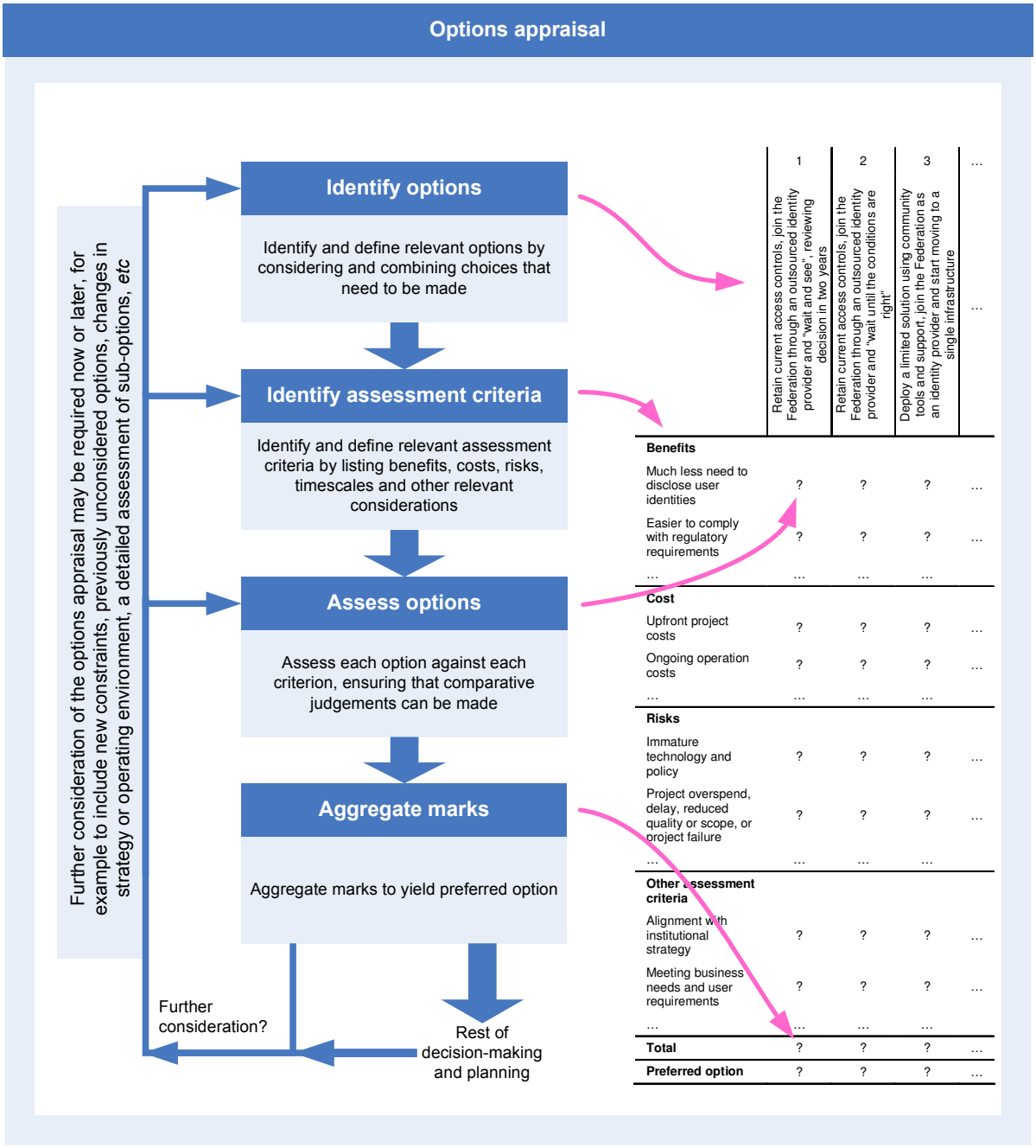


Figure 4-6: options appraisal with exemplars

This page is intentionally blank

5 Affordability

5.1 Introduction

5.1.1 Any proposed investment needs to be affordable and the budget needs to be agreed. Where a range of stakeholders is involved, multiple budgets may need to be agreed before a project can be initiated. If there is financial uncertainty, it may be difficult to secure funding beyond a short horizon. In any case, the proposed budget is competing against other priorities and needs. If the investment is deemed unaffordable it is necessary to revise the intended course of action.

5.1.2 This section addresses "affordability", linking the proposed expenditure to available budget and existing commitments. There is comparatively little information in this section: ensuring affordability is an integral part of all investment decision-making in all organisations and is specific to each organisation. A number of "issues to consider" are set out.

5.2 Questions and content

5.2.1 Questions that must be addressed:

- Is the required budget available to deliver the whole project?
  - What budget(s) will be used?
  - Is this capital or operating expenditure, or both?
  - It the funding available and secure?
  - Is there any contingency?
- If not, can the budget be obtained?
  - Can the scope be reduced or delivered over a longer period?
  - Could funding be sought from other sources?
- What is the cost of not pursuing the preferred cost of action?
  - What other plans and activities are dependent on it?

5.2.2 When writing the business case, the minimum content of this section is:

- a statement of available funding;
- broad estimates of projected through-life cost, broken down by budget-holder where applicable.

5.3 Issues to consider

5.3.1 When assessing affordability of the preferred option it is necessary to consider the following issues:

- **Budget availability**: moving to federated access management requires a range of stakeholder involvement. It is essential to determine which stakeholders are contributing to the budget for the preferred option: whether it is IT Services, Library Services, other departments or a combination. Different budgets will have different processes for managing them and different cycles within which they run. This leads to questions such as: When do budget requests need to be made? When will they be confirmed? For what period(s) are the budget available? What happens to any underspend?

Kidderminster College

Kidderminster College carried out an open-source research and investigation project prior to implementing federated access management to enable Kidderminster to build its' capacity, knowledge and in-house expertise. It was estimated that this project cost Kidderminster approximately £39.5k, and included:

- **research and investigation**: ~1 year FTE of a developer's time (~£25k);
- **staff development**: ~£4k was spent on staff development training courses (*eg* Linux);
- **equipment**: ~£3.5k was spent on specific equipment (*eg* server) to support the project;
- **estates and infrastructure**: other college resources and workspace (~£7k).

- **Cost profiles**: most investments have a "cost profile" that requires, say, a majority expenditure up-front. Checking that the cost profile matches the budget(s) is important.

- **Explicit costings**: often internal costs, particularly staff costs, are not explicitly costed and accounted for. In other institutions, activity based or full economic costing processes may have more formal requirements. Where non-costed resources are needed, it is still necessary to check that they are available, for example: are the required number of staff available at the required times? This issue is considered further under "capacity" in Section 7.

- **Robustness**: the preferred option should be checked to ensure that it is still both affordable and preferred, if the timings and magnitude of costs and savings change from that expected.

6 Commercial aspects

6.1 Introduction

6.1.1 Where it is decided to procure services externally, such as commercial tools or support or an outsourced identity provider, consideration should be given to how this is achieved economically, effectively and efficiently. This section outlines the potential commercial arrangement.

6.2 Questions and content

6.2.1 Questions that must be addressed:

- Can value for money be obtained from the proposed partner or supplier?
  - Are the through-life costs understood?
    - Are likely support costs clear?
    - Are there "hidden costs" like supplier lock-in or restrictive terms and conditions?
    - Is current and future pricing agreed?
- If not, can the project be made attractive to a wider market?
  - Is there sufficient competition to get a good deal?
- What controls on release and use of identity information are there?
  - Are they consistent with institutional strategy?
- Are the skills in place to deal with the commercial aspects?
  - Is it an existing, trusted supplier?

6.2.2 When writing the business case, the minimum content for this section is:

- the procurement approach with supporting rationale;
- the proposed sourcing option, with rationale for its selection;
- the key features of proposed commercial arrangements (*eg* contract terms, contract length, payment mechanisms and performance incentives).

6.3 Guidance

6.3.1 The options appraisal section indicated that there are various commercial options available, for example with respect to service offerings, tools and support. Standard commercial processes can be applied to services procured externally.

6.3.2 One difficulty comes from extent and rate of sector and technology change. The changing access management landscape is likely to lead to a broad and diverse range of offerings. There may be some uncertainty without as much hard commercial information, particularly with some of the more immature offerings. For example, future service offerings and subscription charges, exact support costs and competing offerings may be difficult or impossible to ascertain. Remaining adaptable and working with the supplier may suitable mitigations to this risk.

This page is intentionally blank

7 Achievability

7.1 Introduction

7.1.1 The final consideration is whether the chosen option is "achievable", *ie* can the decision be implemented and subsequent activities completed successfully? If, by review of project plans and discussion, there is uncertainty in this then it may be necessary to modify the plans or even revisit the choice itself. If the answer is "no" or "not at the moment" then clearly further consideration of the intended course of action is required that reflects the institution's current readiness, capability and capacity.

7.1.2 This section addresses the "achievability" of the project and subsequent operation. It looks at what project organisation and actions are required to support the realisation of intended outcomes and desired benefits. Many questions to address are common to any IT-enabled change project.

7.1.3 This section focuses most of those options where change is significant and more challenging; by their very nature, simpler changes are more achievable and need less scrutiny.

7.2 Questions and content

7.2.1 Questions that must be addressed:

- Is the institution ready for the change?
  - Are the pre-requisites in place and dependencies being managed?
  - If not, what needs to be done?
- Can the change be achieved with current capability and capacity?
  - Are the necessary skills and experience available to assign to the project?
  - Is there sufficient assigned and unassigned resource available and ready?
  - Is the organisation able to manage and achieve a technology-enabled change project?
    - Is there a successful track record of such projects?
    - Is there an appetite and organisation culture for the required change?
    - Is there senior management leadership and commitment for the change?
    - Is the project sponsor fully committed and are the stakeholders "on board"?
    - Is there an understanding of and agreement on what will constitute success?
- If not, how can the required capability and capacity be acquired?
- Can the risks be managed?
  - Are stakeholders content with the residual risk?
  - Can another option be implemented if the preferred option fails?
- Does the scope or timescale need to be changed?

7.2.2 When writing the business case, the minimum content for this section is:

- a high level plan for achieving the desired outcome, with key milestones and major dependencies (*eg* identity management or VLE projects);
- the key roles, with a named individual as the project's sponsor;
- outline contingency plans (*eg* addressing failure to deliver service on time);
- the major risks identified and an outline plan for addressing them.

7.3 Is the institution ready for the change?

7.3.1 The changes required for certain options will be minor. For example, to maintain existing access management strategy and subscribe to an existing outsourced identity provider like Athens little preparation is required and assessing readiness is simple.

Dependencies should be included within planning, including directory services deployment, joining federation, *etc.*

7.3.2 For other options, like deploying a single access management infrastructure, the business and technical change will be considerable. Particularly where change will be greatest, it is necessary to assess whether the institution is prepared and ready for the change by assessing whether the pre-requisites are in place, including:

- awareness and understanding across key stakeholders;
- identity management and attribute store;
- entitlement policy;
- regulatory and Federation compliance.

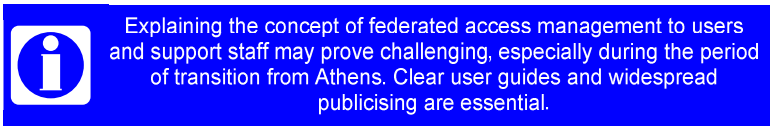
Awareness and understanding across key stakeholders

7.3.3 A typical project to deploy federated access management will involve a growing range of stakeholders as it progresses towards and into operation. The understanding required by these stakeholders will be different and will occur at different times. The project will need to be well explained and a communication plan developed to ensure all stakeholders are told what is required when required. For example, good business and technical understanding is necessary right at the start, in order to make a considered decision, and some of this understanding will need to be passed on to others who are less familiar with the demanding concepts of federated access management. A pilot project might be used to build sufficient understanding.

Kidderminster College

Kidderminster College carried out an open-source research and investigation project prior to implementing federated access management to enable Kidderminster to build its capacity, knowledge and in-house expertise. This has subsequently supported Kidderminster's development and roll-out of its Moodle VLE as well as Shibboleth technology. It was estimated that this project cost Kidderminster approximately £39.5k, and included:

- **research and investigation**: ~1 year FTE of a developer's time equating to ~£25k;
- **staff development**: ~£4k was spent on staff development training courses (*eg* Linux);
- **equipment**: ~£3.5k was spent on specific equipment (*eg* server) to support the project;
- **estates and infrastructure**: ~£7k was spent on other college resources and workspace.



7.3.4 "Change champions" may be required to ensure that the business process changes can occur. If joining the Federation, understanding the rules of membership and any requirements (*eg* for metadata and attributes) and impacts (*eg* on identity management processes) is essential. End users, who may need to know nothing of the concepts, do need to know how to access the services to which they are entitled and where and how to seek help if there are problems.

Cardiff University

Cardiff found that deploying federated access management (using Shibboleth technology) forces an institution to do several things it probably should have already in place, but likely does not (*eg* a comprehensive identity management system, proper directory services and good intra-institution political goodwill).

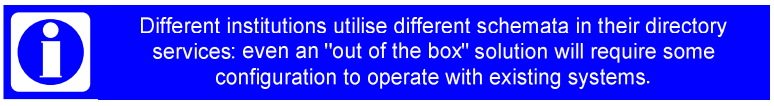
Kidderminster College

Kidderminster considered what information is essential for the changes to be planned and managed properly. For example, teaching staff need to trust the technology and be assured in the robustness of new services; the library needs details on the timings of new/revised services; and, trainers and users need helpsheets to explain the changes and move to new ways of working.

Identity management and attribute store

7.3.5 Federated access management relies on the management and use of identity information, and supply of identity information as attributes. One prerequisite is an attribute store such as directory services (*eg* Microsoft Active Directory, Novell eDirectory and OpenLDAP). Where there is no attribute store, or where it is not appropriate for federated access management needs, one may need to be procured: this is likely to add considerable cost to the option. Further considerations are set out below:

- The attribute store needs to cover all users of services in scope. Where there are multiple legacy directory services it may be possible to deploy meta-directory services that aggregate other directory services. In this instance it is necessary to check for duplication or inconsistencies in identity information.



- The attribute store needs to supply specified attributes to service providers in order to authorise users to have access to the services. The right types of attribute need to be stored: normally a store is populated according to an attribute schema. The definition of the schema needs to support all applications of the attribute schema. Those joining the Federation as an identity provider need to consider four categories of attribute: existing attributes, the Federation's mandatory set, the Federation's recommended set and others as required by particular service providers.

For some (typically larger) institutions, solving identity management issues will be the longest activity and involve difficult organisational and business process change.

- Governance and processes to maintain identity information and the attribute need to be in place. In some cases, automated, centralised processes may make population and changes easy; in other cases it will be a difficult administrative task. It is necessary to check that users are content that their identity provider can release attributes concerning them.

There is a need to solve identity management issues before or concurrently with implementing federated access management. Poor identity management is likely to result in unsuccessful outcomes, and potential issues with resource license agreements.

7.3.6 Effective identity management means the institution is assured that the attributes that are supplied are accurate: if identity information and management is not internally in order then other, external users of federated access management can not be expected to trust the institution.

Entitlement policy

7.3.7 An entitlement policy sets out user entitlements: which users, or categories of user, are entitled to access which services. This is based on user needs and institutional policy (*eg* for internal services) and licence agreements (*eg* for licensed services). Entitlement policy links together much of identity management and access management requirements. Such policy must:

- ensure that all user categories are included; some are non-obvious for institutions with many activities and interests.

It is critical to dedicate sufficient time developing appropriate access policies and user attributes. This needs to be reflected in the planning, and budgeting for adoption.

- ensure that all services are included; this needs to be at a level of granularity that matches the entitlement (*eg* if every user is entitled to access and use an office application set then this can be considered as one service; there is no need for constituent applications each to be a service).

Cardiff University

It took 18 months and significant effort to develop the entitlement policy (and governance processes for maintaining it) and to submit a paper to the University Board to establish institution-wide policy. Hundreds of categories of user were identified and decisions made on University member status, contract status and entitlements for services. Although a project within INSERV it involved extensive stakeholder consultation and discussion.

- match user categories with entitlements to services as per policy and licence. It may be easier with a default access or deny. In some cases it may be necessary to add additional

information or caveats. User entitlements may be easily visualised as a "matrix", like the exemplar below:

Category	Member?	Services			
		S1	S1	...	Sn
Faculty	✓	✓	✗	...	✓
Staff	✗	✓	✓	...	✗
Temp	✗	✓	✓	...	✗
Undergrad	✓	✓	✗	...	✓
...	...				

Figure 7-1: exemplar user entitlements

- agree governance and processes to maintain entitlement policy, as part of good practice and to make it easy to introduce new services and support new user categories in the future.

Regulatory and Federation compliance

7.3.8 An attribute store provides information on users to services. Institutions are bound under data protection legislation to protect personal data. It is necessary to consider data protection issues, and what new or revised processes (*eg* managing permissions for use of data release) are required, when considering use of federated access management. It may be useful to liaise early with data protection officers, or obtain other sources of legal information and advice.[22]

7.3.9 Joining the Federation requires that the institution agrees to and signs the rules of membership. It should be noted that this is a legal contract, and therefore should be clearly understood prior to any commitment to join. The rules of membership set out important areas such as responsibilities, liability and audit. It should be borne in mind that the Federation is simply negotiating authentication and authorisation controls: an institution keeps responsibility for negotiating access to services and ensuring compliance with whatever protection is required.

7.4 Is there capability and capacity for the change?

7.4.1 Deploying federated access management requires sufficient capability and capacity to achieve and manage the change. Deploying a limited, technical solution is less difficult than

22 *Eg* The Federation provides guidance in *Recommendations for Use of Personal Data*, 22 November 2006, available on the Federation website <http://www.ukfederation.org.uk/content/Documents/FedDocs/>. JISC Legal provides legal information on a range of ICT legal issues for the FE and HE sectors, and operates an enquiry service <http://www.jisclegal.ac.uk>.

establishing a single infrastructure. For example, the CM programmes established that a range of technical skills were necessary to deploy federated access management using community tools. Adequate staff need to be assigned to the project through to completion and it is important to consider whether the project can and will be prioritised throughout its lifetime.

7.4.2 Depending on the preferred option, various checks may be necessary to ensure that there is capability and capacity for the change. For example:

- A skills audit to ensure that the necessary technical skills are in place. For example, the SWISH Early Adopter project developed a skills audit for a UNIX Shibboleth Administrator (see the project's final report at <http://www.exeter.ac.uk/swish>).

Cardiff University

Cardiff assessed that it adequate capacity and in-house skills to roll-out Shibboleth technology within the University. Cardiff set up a formal project team, and JISC Early Adopter money enabled a dedicated IT officer to be employed who has now built up significant experience in Shibboleth technology, IDM and directory services.

Kidderminster College

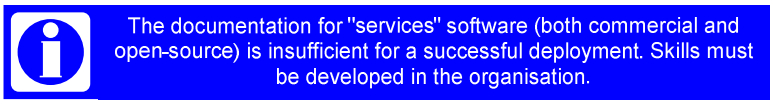
Kidderminster IT Services has a dedicated development team. The team is well resourced, well trained, proactive and confident with open-source software. It was assessed that the implementation of a Shibboleth IdP could be achieved within their current capability and capacity, although some training in new technologies was required.

University of Surrey

Surrey has a lean staffing structure, and does not have extensive in-house technical expertise. The implementation of AthensDA could however be achieved within their in-house capability and capacity, with external support provided by Eduserv when required.

University of Warwick

Warwick has a well-funded and resourced IT Services, with a capable and mature in-house development team, which was well placed to implement the Shibboleth-profile based access management system.



- A technical demonstrator or pilot project to check or build sufficient capability. For example, many of the expertise, to prepare for full adoption and to learn how to exploit effectively the technology to meet business needs and user requirements.

- An assessment of the appetite institutions involved with the CM programmes used their Early Adopter projects to build organisation culture for the intended change and where key stakeholders are committed. Previous business change experiences are likely to be influential in deciding this.

Kidderminster College

One of Kidderminster's aims was to share courses with its regional partners. Kidderminster agreed with the partners the terms of sharing and on the access controls for doing so. For example, the collaboration with the University of Worcester to allow certain students to access Kidderminster's VLE was previously based on Kidderminster provisioning accounts for Worcester's students. Worcester deployed a Shibboleth IdP and agreed the sharing policy (including authentication requirements, metadata exchange, *etc*) with Kidderminster. This required effort and commitment from both institutions.

- An audit of services in scope to ensure that they support federated access management. Services within the Federation will. Others may need some work to enable this functionality.

- An assessment of the managerial capability to deliver a substantial business change project. For example, where complex, large-scale identity and access management projects are running in parallel, perhaps with other projects dependent on the resulting business change, it is necessary to consider whether the expertise exists to achieve the overall "programme" of change.

Cardiff University

Within converged IT and library services, separate responsibilities were assigned for a) developing the infrastructure, and b) implementation and roll-out. This was judged to have worked well since the library have a close relationship with users through inductions and workshops. Changes, and the rationale for changing, was clearly communicated to library staff so that they were aware and understood why the change was happening and how to respond.

7.5 Good practice resources

7.5.1 The following resources may be useful when planning the project and operation:

- The JISC infoNet provides a series of good practice models for the education sector. These infoKits encompass a subject overview, a "how to" guide and other resources. Relevant infoKits are available covering change management, project management, risk management, records management and system implementation. They are available at <http://www.jiscinfonet.ac.uk/infokits/>.

- The OGC provides a range of resources covering programme management ("Managing Successful Programmes"), project management ("PRINCE2") and service management ("ITIL"). These resources are based on the experiences of public sector and contain much useful guidance and information covering, and lessons from, IT-enabled business change programmes and projects. They are available at <http://www.ogc.gov.uk>.

- The case studies within the supplement to this toolkit offer many useful project planning and implementation lessons, and offer links to further resources.

This page is intentionally blank

A Checklist for decision-making

A.1 Access management requirements

A.1.1 This should answer:

a) What (electronic) services are offered and what are their existing access controls?

b) What are our user requirements and business needs for access management?

A.2 Strategic fit

A.2.1 This should answer:

a) Why do we have to change?

b) Are access management requirements currently being met?

c) What strategic drivers are there and does the change fit with institutional strategy?

d) What is the institution's preference for commercial tools (and support) versus community tools (and support) for critical services?

e) To what extent should identity information be controlled within the institution?

f) How many services should be brought together under a single access management infrastructure?

A.3 Options appraisal

A.3.1 Options are identified from the following sets of choices:

a) **Strategic choices**: do not adopt federated access management; deploy a limited federated access management solution; or deploy a single federated access management infrastructure;

b) **UK Federation choices**: do not join the Federation; join the Federation as an identity provider; or join the Federation through an outsourced identity provider;

c) **Deployment options**: using community tools and community support; using community tools and commercial support; using commercial tools and commercial support; or using tools developed in-house and internally supported;

A.3.2 The options appraisal should assess each option:

a) What benefits are available and can be realised?

b) What will the upfront and ongoing costs be and what risks might occur?

c) What assessment criteria (and additional considerations) are necessary?

A.3.3 The options appraisal should lead to a preferred option and course of action.

A.4 Affordability

A.4.1 Which budget will be used? IT Services? Library services? Both? Other?

A.4.2 Is the capital and operating budget profile sufficient given the proposed cost profiles?

A.5 Commercial aspects

A.5.1 Can value for money be obtained from the proposed partner or supplier?

A.6 Achievability

A.6.1 Is the institution ready for the business change and are pre-requisites in place?

a) Is there sufficient awareness and understanding across key stakeholders?

b) Is there effective identity management in place, with an appropriate attribute store?

c) Is there an institutional entitlement policy (covering all users and services)?

A.6.2 Is there capability and capacity for the change?

a) Are there the necessary skills and experience?

b) Can the services in scope support federated access management?

c) Is there the appetite for the intended change and stakeholder commitment?

B Requirements

B.1 Introduction

B.1.1 This annex provides a set of common identity and access management requirements. They are a synthesis of published requirements.[23] An institution's actual requirements will vary and include more detailed requirements.

B.2 Core access management requirement

B.2.1 The core requirement is the ability to manage access to services in a uniform way covering the following four scenarios:

a) Access to internal services, including administrative systems where role-based authorisation may be particularly appropriate;

b) Access to third-party services provided by publishers and other institutions;

c) Inter-institutional use to support shared services (*eg* e-Learning resources and environments across a regional consortium);

d) Inter-institutional use to support dynamic, ad-hoc collaborations (*ie* virtual organisations in e-Research terminology).

B.3 Services

B.3.1 Services that require access controls may encompass network, email, file and print, office and specialist applications, VLEs, electronic resources (including those currently protected by Athens, and those not), repositories, corporate systems, library services, *etc*.

B.4 User requirements

B.4.1 Access shall be permitted to the full range of services for which the user has authorisation, wherever the user or services are geographically located and on whatever user environment is available.

B.4.2 Access management mechanisms shall be as unobtrusive as possible. Access shall be permitted to the full range of services with the minimum number of authentication challenges and with the least possible extra demands on the user.

B.4.3 Logging out from the services shall occur at the end of the user session with the minimum of user interactivity.

B.4.4 Information released about a user's activities shall be compliant with confidentiality and privacy needs.

---

23 Sources include *Sparta: the Second-Generation Access Management System for UK Further and Higher Education: A discussion paper on the requirements*, Alan Robiette, September 2000; *Connecting people to resources: Athens and Shibboleth*, JISC, April 2005; and, *Identity Management*, RUGIT Report, Tim Phillips, October 2006.

B.4.5 Access management infrastructure shall enable personalisation and customisation of users' experiences where desired.

B.5 Institutional requirements

B.5.1 Access management infrastructure shall support other business needs and reporting.

B.5.2 Access management infrastructure shall keep the administrative burden of maintaining credentials, such as usernames and passwords, as low as possible. In general, operational and support costs shall be minimal.

B.5.3 Access management infrastructure shall support and be compliant with security policy and relevant legalisation. This will often include supporting role-based access policies.

B.5.4 Access management infrastructure shall provide levels of availability and resilience in line with institutional policy.

B.5.5 Access management infrastructure shall use open and vendor-independent standards.

B.5.6 Access management mechanisms shall interface with relevant legacy systems such as authentication and sign-on mechanisms and sources of identity information.

B.5.7 Access management infrastructure shall interface with a range of local environments.

B.6 Service provider requirements

B.6.1 Access management infrastructure shall permit access to services only to *bona fide* members of those institutions who are entitled to use it and that any other agreed conditions are adhered to.

B.6.2 Audits shall be permitted to monitor the implementation of access policies. These may require individual users to be identified.

B.6.3 Access management infrastructures shall permit the collection of management statistics as set out in usage policy, licence conditions or other agreements.

B.7 Identity management requirements

B.7.1 Effective identity management is a pre-requisite for access management. Identity management requirements include the ability to:

a) Keep track of users and their role(s) in the institution;

b) Maintain accurate records;

c) Manage accounts in an accurate and timely manner;

d) Meet regulatory and legislative requirements (*eg* Freedom of Information Act, Data Protection Act, Human Rights Act).

B.7.2 Users will increasingly want to carry their identities from institution to institution.

This page is intentionally blank

C Lessons identified

C.1 Introduction

C.1.1 A number of lessons from UK and international activities from the access management arena have been identified. Some of these lessons, particularly those from the CM programmes, are synthesised, categorised and presented below. References are provided in footnotes.

C.1.2 Further lessons, within the context of projects, are set out in the case studies supplementing this toolkit.[24]

C.2 Lessons

Strategic fit

C.2.1 Successful implementations are likely to be driven by institutional strategy and business-critical services.[25]

Identity management

C.2.2 There is a need to solve identity management issues before or concurrently with implementing federated access management. Poor identity management is likely to result in unsuccessful outcomes, and potential issues with resource license agreements.[26,27,28]

C.2.3 There are substantial opportunities and resulting benefits for larger institutions to integrate their identity and access management infrastructures.[26]

C.2.4 There is often no clear owner of the identity management problem within institutions. For institutions with such owners, there is little consistency in their position or role. This can be an issue with addressing identity and access management.[26,27]

C.2.5 For some (typically larger) institutions, solving identity management issues will be the longest activity and involve difficult organisational and business process change.[26,27]

Project planning

C.2.6 Liaison with a wide range of stakeholders will be required, including: records departments, library, commercial companies, partner institutions, *etc*.[26,27,29]

C.2.7 Liaison with institutions who have implemented the same access management system can help identify many of the potential issues with the project.[30]

---

24 *CC297D002-1.0 federated access management: case studies supporting the business case toolkit*, 18 June 2007.

25 *WM-Share - Shibboleth and Repositories of Teaching Content Report*, July 2006.

26 *CM programmes: component project outputs*, CC253D010-1.0, Issue release 1.0, 17 November 2006.

27 *SWISh Draft Final Report*, June 2006.

28 *ASMIMA Final Report*, 31 March 2006.

29 *The Learning Matrix Final Report*, Draft March 2006.

C.2.8 A diverse technical skill-set is needed to implement a complete system: expertise is required with web applications, networking, single sign-on systems, firewalls, Unix, PKI, Java, XML, *etc*.[26,29,31]

C.2.9 Non-technical factors are important, including organisational, policy, commercial, recruitment, *etc*.[26,25,32,33,28]

C.2.10 Dependencies should be included within planning, including directory services deployment, joining federation, *etc*.[26]

C.2.11 There will be inevitable changes, including new software versions, configuration demands, *etc*.[26,34]

C.2.12 Shibboleth installations led by e-Learning teams typically underestimate the time required and technical complexity of installing Shibboleth.[35]

C.2.13 Support from an experienced team is advantageous.[25]

C.2.14 Non-IT led projects may be dependent on the IT service of their institution to prioritise and provide a Shibboleth infrastructure.[32,34,36]

C.2.15 Using a test environment provides confidence when rolling out production services.[30,37]

Policy development

C.2.16 It is critical to dedicate sufficient time developing appropriate access policies and user attributes, in order for deployments to succeed. This needs to be reflected in the planning, and budgeting for adoption.[26,29,38,39]

C.2.17 Risks to the key institutional information assets are rarely recognised or managed. There is a perception that this will become increasingly important. Not all assets have access controls at present.[26]

C.2.18 It is expected that implementing single sign-on will cut down password proliferation but increase the risk for any single password loss. Therefore, passwords will continue to be a weak link.[26]

---

30 University of Surrey case study within the supplement to this toolkit, CC297D002-1.0.

31 *ShibboLEAP Project Final Report*, Joint Main Report, May 2006.

32 *WM-Share Shibboleth Early Adopters Final Report*, July 2006.

33 *UNISA Final Report*, 2nd Draft, 6 April 2006.

34 *Shibboleth in Higher Education*, 10 May 2006.

35 *Review of JISC Distributed e-Learning Regional Pilots*, Interim report, March 2006.

36 *EPICS Final Report*, March 2006.

37 University of Warwick case study within the supplement to this toolkit, CC297D002-1.0.

38 *EPISTLE Final Project Report*, Undated.

39 Cardiff University case study within the supplement to this toolkit, CC297D002-1.0.

User experience

C.2.19 Users may use passwords as part of personal, unofficial access controls. Coarse-grained authentication mechanisms (*eg* a single password) may lead to user inconvenience.[26]

C.2.20 The security of "silent" authentication failures must be balanced against the improved user experience of informative failure messages.[26]

C.2.21 Explaining the concept of federated access management to users and support staff may prove challenging, especially during the period of transition from Athens. Clear user guides and widespread publicising are essential.[28,30,33,39]

C.2.22 Federated access management to a VLE or repository between institutions is especially beneficial where institutions share the teaching of some courses.[25]

C.2.23 Library induction sessions are the main opportunity to get the "resource use" message through to users. Library staff need to be trained in time for running these sessions.[39,40]

Technical factors

C.2.24 Different institutions utilise different schemata in their directory services: even an "out of the box" solution will require some configuration to operate with existing systems.[29,38]

C.2.25 The documentation for "services" software (both commercial and open-source) is insufficient for a successful deployment. Skills must be developed in the organisation.[31,41]

C.2.26 There are no interfaces for first line support staff to resolve problems with a Shibboleth server, it must be escalated.[33]

C.2.27 The ability to generate usage accounting information must be considered.[26,28,33]

C.2.28 Shibboleth IdP servers need to be accessible from the Internet, with an Internet-facing IP address, or appropriate firewall pass-through.[38]

C.2.29 Compiling Shibboleth on various platforms can prove challenging.[29,42]

---

40 Kidderminster College case study within the supplement to this toolkit, CC297D002-1.0.

41 *EMSS Final Report Draft*, 27 March 2006.

42 *RIPPL Final Report*, 27 March 2006.

This page is intentionally blank