

Access Management Systems for  
Electronic Resources in  
U.K. Higher Education:  
a comparative evaluation

by

Ian J. Tilsed, BA

A dissertation submitted to  
Department of Computing  
The Business School  
UCE Birmingham  
in partial fulfilment of the requirements for  
the Degree of Master of Science

UCE Birmingham  
September 2006

## **Abstract**

The aim of this dissertation is to identify and assess the current and proposed access management systems for electronic resources in the U.K. higher education sector and to identify the policy issues that arise from the implementation of those systems. A further aim is to identify a set of criteria by which access management systems may be evaluated.

Access management systems for electronic resources have been in existence for some time, in the form of such approaches as IP address filtering and proxies. However, the services provided by Eduserv Athens, together with the advent of Shibboleth as the proposed national access management system, suggest that the topic is ripe for further study and evaluation.

A mixed methodological approach was employed for this study, utilising a survey, backed up by interviews and qualitative analysis, to assess the various systems under review. Furthermore a set of criteria, first employed in 1998, was identified as a framework for analysis.

The research findings indicated that those access management systems based on existing institutional accounts, rather than the issuing of additional logins, were closer to the ideal of a perfect access management solution. The research also identified the tensions between privacy and accountability as a major area for policy review.

The framework for analysis performed well, although the weighting of detail within the various criteria was identified as an issue for further methodological study. Questions were also raised about the appropriate methodological tools by which the analysis framework could be applied.

# Contents

	<b>Page</b>
<b>Abstract</b>	<b>1</b>
<b>List of Contents</b>	<b>2</b>
<b>List of Tables and Figures</b>	<b>5</b>
<b>Acknowledgements</b>	<b>6</b>
<b>Abbreviations &amp; Definitions</b>	<b>7</b>
<b>Chapter 1 Introduction</b>	<b>8</b>
1.1 Aims	8
1.2 Objectives	9
1.3 Scope	9
1.4 Benefits and Justification	10
1.5 Organisation of the Thesis	10
<b>Chapter 2 Literature Review</b>	<b>13</b>
2.1 Nature of Material	13
2.2 Definitions and Assumptions	13
2.3 Current Approaches to Access Management	15
2.4 Recent Developments in UK Higher Education	20
2.5 Next Generation Access Management Shibboleth	24
2.6 Policy Issues	25
2.7 Summary and Areas for Further Research	26
<b>Chapter 3 Methodology</b>	<b>27</b>
3.1 Methodological Approach	27
3.2 Evaluation Criteria	29
3.3 Research Design	32
3.3.1 Range of Systems	32
3.3.2 Perspective	32
3.3.3 Sample	33
3.3.4 Obtaining the Data	34
3.4 Presenting the Results	40

<b>Chapter 4</b>	<b>Research Findings</b>	<b>41</b>
4.1	The Sample	41
4.2	Comparative Evaluation	43
4.2.1	Feasibility and Deployability	44
4.2.2.	Authentication Strength	45
4.2.3	Granularity and Extensibility	46
4.2.4	Cross-Protocol Flexibility	48
4.2.5	Privacy Considerations	48
4.2.6	Accountability	49
4.2.7	Collection of Management Data	50
4.2.8	Overall Assessment	51
4.3	Priorities in an Access Management System	53
4.4	Summary	54
<b>Chapter 5</b>	<b>Discussion and Analysis</b>	<b>55</b>
5.1	Access Management Systems	55
5.1.1	Athens Access Accounts	55
5.1.2	Athens Personal Accounts	56
5.1.3	AthensDA	57
5.1.4	Shibboleth	59
5.1.5	Overview	60
5.2	Evaluation Criteria	60
5.3	Policy Issues	62
5.4	Summary	64
<b>Chapter 6</b>	<b>Conclusion</b>	<b>65</b>
6.1	Access Management Systems	65
6.2	Evaluation Criteria	66
6.3	Methodology	66
6.4	Summary	67
<b>Chapter 7</b>	<b>Reflections</b>	<b>68</b>
	<b>References and Bibliography</b>	<b>69</b>

**Appendix A** Survey Design

**Appendix B** Example E-Mail

**Appendix C** Interview Schedule

**Appendix D** Roles and Allegiances: Open Responses

**Appendix E** Survey Results Tables

**Appendix F** Priorities in an Access Management System: Table

**Appendix G** Comparative Analysis: Table

**Appendix H** Respondent Comments

## List of Tables

		<b>Page</b>
Table 1	Respondents per Access Management Approach	43
Table 2	Overall Rating of all Four Approaches to Access Management	52
Table 3	Ranking of Factors / Facility in Order of Importance	53

## List of Figures

		<b>Page</b>
Figure 1	Survey Respondents: Role	42
Figure 2	Survey Respondents: Departmental Allegiance	42

## **Acknowledgements**

I would like to thank all the academic and administrative staff at UCE Birmingham who provided advice and support throughout my dissertation period and my earlier studies.

I would also like to thank the library staff at UCE Birmingham and the University of Exeter for their role in facilitating access to the research material for the research.

I am grateful to the University of Exeter for providing financial and study support, without which this period of study would not have been possible.

I am also very grateful to my family, friends and colleagues who provided encouragement and advice through my studies, especially during times when life and work pressures seemed overwhelming.

## Abbreviations & Definitions

<b>Abbreviation</b>	<b>Definition</b>
API	Application Programming Interface
AthensDA	Athens Devolved Authentication
ARP	Attribute Release Policy
CNI	Coalition for Networked Information
ID	Identity
IP	Internet Protocol
ISP	Internet Service Provider
JISC	Joint Information Systems Committee
JMU	JISC Monitoring Unit
LDAP	Lightweight Directory Access Protocol
LMS	Library Management System
SAML	Security Assertion Markup Language
SD	Service Delivery
SSO	Single Sign-On
SWISh	South West Implementation of Shibboleth
X.509	A digital certificate standard



# 1. Introduction

The nature of information provision in library and information services has changed dramatically during the last ten years, with a transition from printed to electronic resources or, more commonly, the adoption of a mixed economy, that Rusbridge (1998) terms a 'hybrid library'. Moyo (2002 p. 49) rightly identifies that the focus for libraries, now, is 'on the information rather than the source, and consequently on access rather than ownership' and stresses that this has 'heightened the need for libraries to set up relevant technological infrastructures to permit global access to electronic resources'. The process of implementing such solutions for shared and licensed access to network resources has led to what Lynch (1998a p. 1) identifies as the emergence of 'authentication and access management...as major issues which threaten to impede progress'. Lynch is not alone in further identifying that the 'challenge of cross-institutional access management is not to set up barriers to access' (Bordeiau, 2000 p. 112). This, together with the ever-increasing use of electronic resources and increasingly diverse patterns of study and attendance in higher education, means that access management in the UK is undergoing extensive development.

This study will address this changing access management landscape by carrying out the research as outlined below.

## 1.1 Aims

1. To assess current and proposed access management systems in the UK higher education library sector.
2. To establish a set of criteria by which access management systems may be evaluated.
3. Identify policy issues that arise from the implementation of access management systems.

## **1.2 Objectives**

1. To identify current and proposed access management systems.
2. To identify a set of criteria and a system for evaluating access management systems.
3. To comparatively evaluate the systems using the identified criteria.
4. To present a summary of the strength and weaknesses of the systems.
5. To critically evaluate the criteria used in the study and to suggest improvements.
6. To critically engage with any policy issues that arise during the implementation of the systems.
7. To identify and recommend priorities for the future development and implementation of access management systems.

## **1.3 Scope**

To some extent the UK, due in part to the ongoing implementation and development of Athens (Eduserv Athens, 2006a) and associated projects, has been one of the leaders in the development of access management systems, although the international community, particularly the U.S. and Europe, are active in research.

In the UK, the recent decision by JISC (2006a) to adopt Shibboleth as the basis for access management for both further and higher education will mean significant changes to the current situation, in both technical approach and functionality. The new service is intended to replace the Eduserv Athens service as JISC supported approach to access management by 2008, although funding models for the continued provision of Eduserv Athens beyond that date are under review.

Given the extensive change in access management that is beginning to take place in the UK, this study will address only those access management systems that are currently in use in UK higher education, namely Eduserv Athens in its various forms, and the next generation access management system, based on Shibboleth and recently chosen by JISC (2006a).

#### **1.4 Benefits and Justification**

Access to a wide variety of electronic information by UK higher education sector has grown to such significance that it is now an integral part of the modern university information environment. However, facilitating access to those electronic resources has become a major challenge, in part owing to the expectations of the modern student and researcher. At a time when significant financial resources are being invested in the move to a Shibboleth solution by JISC and the rest of UK higher education, there is a clear need for a comparative review and evaluation of both the access management systems currently in use and that identified as the replacement. This is all the more important for the information and library community who have, and will continue to have, an integral role in administering such systems. It is hoped that such a comparative evaluation will inform both the users and developers of access management systems, in part through the publication of appropriate material. It is intended that such an evaluation will also contribute to, and encourage, discussion of the policy issues, with particular reference to those of privacy and accountability.

#### **1.5 Organisation of the Thesis**

In order to complete the research, and achieve the aims and objectives as outlined, the thesis has been structured to include the following chapters: introduction, literature review, methodology, research results, discussion and analysis, conclusions and reflections.

The literature review outlines the technologies and issues inherent in managing access to electronic resources, identifies the nature of the material and traces the recent development of access management systems. It also identifies the major non-technical issues that need to be addressed in any discussion, such as the issue of privacy.

The methodology chapter outlines the general principles of both quantitative and qualitative analysis and then sets out in detail the multi-method approach used in this study, detailing the reasons for such an approach. It also identifies the evaluation criteria, based in part on a key text identified in the literature review, and highlights areas of strength and weakness in the approach.

The research findings are presented and analysed in the following chapter. Tables and graphs are used to present quantitative data and to relate the results of the qualitative analysis to the research questions. Limitations in the research approach are identified with respect to particular aspects of the study.

The discussion and analysis chapter relates the research findings to the stated objectives of the study and discusses the extent to which the findings allow conclusions to be drawn about the issues.

The concluding chapter draws on the preceding chapters of the thesis. It evaluates the success of the research, identifies what has been learnt from the research process and considers the future for access management systems in UK higher education.

This is followed by a reflective chapter, where the research process and experience are reviewed, and successes and weaknesses identified.

## **2. Literature Review**

The aim of this literature review is to outline the nature of access management for electronic resources in UK higher education by reference to relevant literature, including academic articles, reports and project documentation. The review will trace the recent process of change from earlier approaches, like IP source address filtering, to the newly proposed solution based on Shibboleth, making reference to evaluative material with a specific view to identifying criteria that can be used in critical assessments in subsequent chapters. This review does not intend to provide a comprehensive overview of all writings on access management, nor does it intend to supply overly detailed technical information about the various systems. Rather it focuses on the current and proposed solutions for UK higher education from the perspective primarily of those would be responsible for their implementation and administration.

### **2.1 Nature of Material**

Whilst there is a wide variety of material relating to the 'hybrid' or 'digital' library and the delivery of services to distance or remote users, dealing often in passing with access issues, there is less material dealing with access management per se (although with the advent of Shibboleth this is changing). The main body of literature consists of journal articles from 1996, together with project materials (from ANGEL, GLAM, HeadLine and others), documents from solution providers (such as Eduserv Athens) and reports from bodies like the British Library, the Joint Information Systems Committee (JISC), the Coalition for Networked Information (CNI) and Internet2. The fast pace of change, together with developments from Library Management System (LMS) suppliers, also means that news may be found in trade journals and newspapers.

### **2.2 Definitions and Assumptions**

In 1998 the CNI, under the leadership of Clifford Lynch, drafted a discussion paper on authentication and access management and released it to its members for

review. Following extensive discussion it was then revised and published as a 'White Paper' in April 1998 (Lynch, 1998a). This paper, hereon referred to as the 'White Paper', forms the basis for much of the current discussion and offers definitions and a terminology that seem to have been universally accepted since.

Access management is strictly a term that describes a system that makes use of both authentication and authorisation so as to provide access to a networked resource. Robiette (2000) defines authentication as the 'process of confirming a link between a person and his or her identity; in other words the process of establishing...that the person operating a networked session is the person to whom the electronic identity is used', although Lynch (1998a p. 3) notes that:

Names need not correspond to the usual names of individuals in the physical world. A user may have the rights to use more than one name: we view this as a central philosophical assumption in the cross-organizational environment.

Authorisation is defined by Robiette (2000) as 'the process of linking the electronic identity to the set of resources to which the person in question has been granted access'. For example a student user, once authenticated, may be authorised to access an online medical database, but they may not be authorised to access a subset of medical images unless they are a medical student.

The scope of recent access management material also generally abides by a further statement by Lynch (1998a p. 2), namely that the focus is on 'group licences' where additional constraints like concurrent usage are applied, rather than on 'transactional models' where individuals enter into more of a business relationship with the resource provider.

A further significant contribution to overall discussion of access management arose from a workshop report by the US-based Digital Library Federation. This report (Arms, 1999) identified five key properties 'for access management systems

that would make them acceptable to users and libraries while respecting the rights and interests of authors and publishers'. As Paschoud (2004 p. 148) has noted, despite a great deal of activity since this report, there has been no improvement on these priorities. As such, and given their importance as the best available working definition of the aims in access management, the five priorities (Arms, 1999 p. 25) are quoted below in full:

1. *Simplicity*. The less complex a system of access management, the more readily it can be adopted technologically and organizationally, and more acceptable it is to all involved in its implementation.
2. *Privacy*. Systems that manage access to the cultural record must protect the privacy of users from detailed tracking and disclosure of use. User privacy must not be compromised.
3. *Good faith*. Agreements on access to scholarly information rely on trust among the parties involved. Users and providers would each prefer to depend, in an access management system that implements these agreements, on reasonable barriers against abuse rather than complex restrictions that inhibit use.
4. *Trusted intermediaries*. Intermediaries play an essential role in providing access to the cultural record as parties trusted by both users and providers and as efficient aggregators of distribution and usage. System design must take the role of intermediaries into account.
5. *Reasonable terms*. Access management systems and license agreements must recognise the distinction between access and use. Overly tight control of access to a resource may impose inappropriate constraints on its use, especially in teaching and research contexts. The most useful system will not limit access to specific user groups known in advance to be interested in a resource but will be reasonably open to serving unlikely users whose curiosity and research interests may lead them in directions not predicted by those responsible for making the agreements or designing the systems.

### **2.3 Current Approaches to Access Management**

For academic libraries there is a constant balance to be maintained in relation to electronic resources. The licensing of online services and making those resources available to the learning, teaching and research communities is a key role.

However, the tension lies in:



adhering to their legal and contractual responsibilities to publishers (to limit access to only those users covered by license terms) and to users (to protect the privacy of personal information registered with them), and to carry out that fundamental function of a library: to offer users the easiest possible path to the information that they need. (Paschoud, 2004 p. 149)

It is evident from the literature that there are three main approaches to access management at the current time – IP filtering (based on computer network addresses), proxies (through which requests for online material may be routed, to appear as if they originate from another network location), and credential-based systems (commonly user ID and password). A fourth method, the furtive approach of word of mouth for a hidden resource, is discounted, owing to modern licensing obligations.

IP filtering is where ‘the service provider limits access to http requests from machines with an IP address within a range registered by the host institution’ (CANDLE-Athens, 2002). Commonly an institutional network consists of a static range of IP addresses that usually corresponds with the networked workstations in a particular place, such as a campus. As such, this method is often used to control access to resources where the licence permits only access from users on campus or physically located in a particular building (such as a Library). However, there are two main problems with this method. As Paschoud (1999b p. 17) and others (Lynch, 1998a p. 13; Moyo, 2000 p. 54; Bordeiau, 2000 p. 116) point out, it is possible to ‘fake’ an IP address and, more importantly, it also denies access to legitimate users who may not be accessing the resource via an institutional Internet connection. Furthermore, it may permit access from users who can gain access to a building or network but who may not be members of the subscribing institution. Owing to its ease of implementation, IP filtering is often used where other approaches are clearly more appropriate. This method therefore defines access by location, rather than by membership of the subscribing institution.

The use of proxies addresses the second problem of IP filtering, in that distance users access a proxy server at their own institution, which authenticates the user against an internal database and passes information requests to the resource with the IP address of the proxy rather than the user's own Internet Service Provider (ISP). However, Lynch (1998a p. 16) and Goerwitz (1998) correctly identify that there are two different types of proxy services – mechanical proxies (which use facilities implemented in the http protocol and require the user to configure their browser to pass all http requests via the proxy server, from where they are then retransmitted onto the destination host) and application-level or gateway proxies (where an application, such as a library catalogue, forwards requests without using protocol mechanisms and without requiring browser configuration changes). In both cases, however, the proxies are often tied to an internal authentication and authorisation system in order to manage access to them, and both still utilise an element of IP filtering – although not to the detriment of the user, as before.

Proxies are not without their problems however. In the case of mechanical proxies Breeding (2001 p. 53) notes that the need for configuration changes to users' web browsers can be daunting and consequently a barrier to access. In addition, a failure to correctly configure a proxy can lead to unauthorised use of resources, particularly if the proxy does not demand authentication of users. Some high profile cases, such as that involving JSTOR (Carnevale, 2002), have highlighted the dangers of incorrect proxy configuration. Integral (application level) proxy modules for library management systems are now commonplace, but the implementation of such systems, whilst not involving the end user, can be challenging for systems staff (Bordeiau, 2000 p. 117).

The credential approach to access management is one area where opinions are mixed, in part owing to varied practices worldwide. In this approach the user deals directly with the networked resource – whether via an ID and password or, less commonly, via digital certificates. Leaving to one side the technical discussion about the transmission of such data (Lynch, 1998a p. 19), it is recognised that users are familiar with usernames and passwords and, often remembered, they can be very mobile (although this can be a problem as well as an advantage). However, if the account details are specific to a user, transactions are unlikely to

be anonymous, but rather pseudonymous (a user may be identified with a persistent but arbitrary identifier like user1) or identified. Furthermore, Lynch (1998a p. 19) notes that:

probably the greatest weakness of this approach is the dependency on each resource operator to protect userid/password pairs, and the danger of systemic compromise due to a security failure on the part of the single resource operator.

The use of username and password is particularly familiar in the UK due to Eduserv Athens, an access management system that has served higher education since 1995 (Eduserv Athens, 2006). Whilst Athens was perceived by many as a transitional or medium term solution for the UK, in part owing to its 'reliance on proprietary API (Application Programming Interface) rather than an existing set of industry standards' (Eaton, 1998 p. 15), it has been regarded as a successful, implementation of a national solution (in part owing to its central funding by JISC on behalf of higher education). Indeed, the service maintains the credentials of over three million Athens users and controls access to over 260 electronic resources, permitting access from any location and at any time.

As Norris (2004 p. 278) has detailed, Eduserv Athens offers access management functionality in several forms. The most widely used is what is commonly called 'Classic Athens'. This is fundamentally a central repository of organisations, usernames and passwords with associated rights, offering devolved account management facilities to organisations to create and manage user accounts and allocate rights to individual usernames. Publishers of electronic resources outsource the management of user accounts, licensing their own access to Athens (and the use of the proprietary software components involved) for an annual fee. To the user this means that one Athens username and password can be used to access a wide range of resources. For the institution the main administrative burden is the creation of the usernames and passwords – these can be created manually by an Athens site administrator, by allowing users to self-register from a restricted IP address range, or via bulk uploads from another source, such as a

student records system (Norris, 2004 p. 278). Two types of account are possible within this system – an access account and a personal account. Access accounts are typically site-wide or departmental accounts, where resource access is based on the correct username/password and sometimes on the user's IP address as well (and thus not appropriate for distance users); they can also be used by users to create personal accounts. Personal accounts are specific to each user, are not bound by any limitations of IP address and are the most common account type.

Eduserv recognised the burden of creating and managing Personal Athens accounts and subsequently developed a system by which organisations could devolve or federate authentication to their own local authentication services, such as LDAP Directory Service. This service, known as AthensDA (Athens Devolved Authentication) was launched in 2003 and has since been adopted by over sixty UK higher education institutions. By integrating with a local authentication system:

AthensDA allows an organisation to maintain a single set of credentials for a user, and for that user to be authorised for access to online services depending on permissions defined by the user's organisation. Hence AthensDA facilitates single point administration of user credentials allowing the user access to both local and external services through SSO. Additionally, AthensDA improves security by ensuring that the user is authenticated at his "home" organisation; and thus the user credentials are not visible to any third party. (Eduserv Athens, 2006b)

It is important to note that it is possible for a user to access a protected resource via AthensDA without having any real appreciation of the process or the actual software. This devolved authentication solution can be incorporated into the institutional online presence without any obvious reference to Eduserv. With the user entering their own local login credentials, their perception of the service may be that it derives from their own institution, rather than from a third party installation. This poses a challenge when undertaking any assessment of a user's view of devolved authentication solutions.

Whereas Athens simplifies access by centralising authentication for many networked resources, there are still some services that rely on their own usernames and passwords. Lynch speaks for many when he writes that ‘large numbers of passwords and userids are extremely unfriendly and confusing for users’ (Lynch, 1998a p. 20). Some commentators have gone so far as to suggest that thirty per cent or more of all help desk calls are those from users who have forgotten their passwords or whose passwords have expired (Clark, 2003).

Although Lynch (1998a p. 20) and others (Robiette, 2001a) discuss client-side certificate-based credentials, it is evident from the literature that this form of access management is still very much under development and should not be considered as current practice.

## **2.4 Recent Developments in UK Higher Education**

To some extent the UK, in part due to the implementation and development of Eduserv Athens and associated projects, has lead the way in the development of access management systems, although the international community, particular the U.S. and Europe, are active in research (MAMS, 2006; NISO 2005; SWITCH, 2006; TERENA, 2004). UK developments have been, and continue to be, driven by JISC, which currently funds Eduserv to run the Athens system as a national access management system for UK further and higher education. Over the last six years considerable effort (and money) has been invested by JISC (and partners) in exploring access management models and solutions for the future. As much of the recent technical developments have been closely associated with the various JISC programmes, it is pertinent to trace the path that has brought UK higher education to where it is today in relation to access management.

In 2000, the JISC Committee on Authentication and Security issued a discussion paper on the requirements for a second generation access management system for UK further and higher education (Robiette, 2000). Whilst recognising the

success of Athens, the paper explored the issues from a range of perspectives and laid some important groundwork for later developments. Among the conclusions was a commitment to the separation of authentication and authorisation, a belief that the authentication of the individual should be the responsibility of the institution concerned, and that authorisation should be nationally managed in relation to nationally licensed resources.

In April 2002 JISC issued two papers, one a discussion paper on proposals for middleware for the JISC information environment (Robiette, 2002b) and the other a consultation of the future of authentication for JISC services (Robiette, 2002a). The former paper, whilst a direct follow-on from the Sparta paper of 2000 (Robiette, 2000), engaged not only with authentication but also the wider development of generic middleware architecture (software that connects two otherwise separate applications) capable of supporting a wide range of user environments and applications. The latter paper, whilst acknowledging the recent introduction of Single Sign-On (SSO) functionality within Athens, noted that Athens did not satisfy the requirements identified earlier in the paper. Indeed, the paper noted that it 'would only take the JANET connection to be down for local authentication to be disabled' and set out arguments for a national scheme to be based on digital (X.509) certificates (Robiette, 2002a).

Subsequently JISC issued a funding call for an access management service (JISC, 2002a), noting that the contract for the current service (Athens) was to expire on 31 July 2003. The new contract was to run for three years in the first instance, with an option for a further two year extension. Eduserv subsequently won the contract and Athens continued as the national access management system for further and higher education (Eduserv, 2003).

Also in 2002 JISC announced funding for eleven projects under its Authentication and Authorisation Programme, in an attempt to advance practical understanding of the latest developments in access management (JISC, 2002b). The projects

explored authentication via digital certificates (JISC, 2002c) and examined emerging solutions for authorisation (such as Shibboleth , PAPI , Akenti and others).

In 2004 JISC announced a major funding initiative of £6.6 million in the area of core middleware (JISC, 2004d), defining middleware to be the 'process of helping education institutions to connect people to resources'. Fifteen projects were funded under four themed areas – technology development, grid-oriented development, portal development, and inter-institutional collaborations (JISC, 2004e).

In late 2004 JISC clarified the future position of Eduserv Athens and announced that it had 'begun work on a solution with the development of a next generation access management system based on Shibboleth technology' (JISC, 2004c). It is noteworthy that JISC, by selecting Shibboleth, moved away from the notion of using X.509 digital certificates in the form (client-side) first proposed in 2002 (Robiette, 2002a), though digital certificates still remain an integral part of the Shibboleth solution, albeit server-side. At the same time a useful summary of the current situation regarding access management was published as part of the planning documents for the Core Middleware Programme (JISC, 2004f). This document noted that 'the current Athens technology does not meet all the emerging access management needs of the community' and identified three areas to be addressed:

- *Use of centralised databases of information* – recognised as appropriate for third party resources but less so for the management of internal resources.
- *Athens is a proprietary system and has a limited international take-up* – identifying a concern about the 'locking in' of institutions and resource providers to one system.

- *New requirements* – noting the lack of flexibility in Athens to address all of the requirements of the community, ‘particularly in terms of inter- and intra-institutional work and collaborative working’ (JISC, 2000f).

The paper went on to recognise the importance of separating the technology from the support service offered by Athens, and noted that Shibboleth could only be compared on a technological level - an important distinction that highlights one area of concern regarding the next generation solution.

However, despite the commitment to move forward with Shibboleth developments, JISC did confirm that:

Eduserv Athens access and identity management service is playing a major part in this development. It is expected that as the new technology is launched, it will work along side Eduserv Athens, ensuring that users are given the simplest route to any resource, internal or external. (JISC, 2004c)

In late 2004, JISC embarked on the deployment of the Shibboleth technology from Internet2 (2006a). A call for proposals from institutions to be ‘early adopters’ of Shibboleth was issued (JISC, 2004g), which formed the basis for the Core Middleware Infrastructure Programme, and 21 projects were eventually supported

In early 2006 JISC (2006a) formally confirmed the adoption of access management technologies based on Shibboleth and the launch of its UK Access Management Federation (an essential element of the system architecture) later that year. It also confirmed that the central funding model for Eduserv Athens would be revised by the summer of 2008, with the expectation that institutions would have moved to one of the Shibboleth implementations by that time (JISC, 2005). As part of the deployment, JISC identified the need to work closely with the



resource providers to ensure that the services are available via Shibboleth. JISC also embarked on a major educational campaign, publishing guides for the various stakeholders in the community (2006c, 2006d, 2006e, 2006f), although evidence suggests that much work remains to be done (Tilsed & Johnson, 2006, p. 15).

## **2.5 Next Generation Access Management: Shibboleth**

To some extent, the Shibboleth solution bears some similarity in approach to that utilised in AthensDA – namely that the authentication of a user is the responsibility of the institution. As Paschoud (2004 p. 152) agrees, Shibboleth is not a method of authentication. Indeed, Shibboleth adopts the separation of authentication (undertaken by the home institution) from authorisation (undertaken by the resource provider), thereby meeting one of the early requirements defined by JISC (Robiette, 2000). Internet2 (2006a) offers the following definition:

Shibboleth is standards-based, open source middleware software which provides Web Single SignOn (SSO) across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.

Cantor and Erdos (2002 section 2.2), in their original architecture documentation, defined the problem that Shibboleth is designed to address:

Shibboleth aims to detangle the management of users at cooperating institutions by ‘federating’ administration. In federated administration, a resource provider leaves the administration of user identities and attributes to the user’s origin site. The resource provider relies on the origin site to provide attributes about a user (possible but not necessarily including a username) that the provider can use in making an access control decision when the user attempts to use a resource.

This literature review will not provide a technical explanation of the Shibboleth solution (see Needleman (2004 pp. 252-253), Paschoud (2004 pp. 152-156) and Internet2 (2006b)), but one of the key principles is ‘allowing user choice in what

information gets released about the user and to which site. Thus the job of balancing access and privacy lies ultimately with the user, where it belongs' (Cantor & Erdos, 2002 section 2.2). Shibboleth is an open source development, utilising the international SAML protocols, that separates authentication from authorisation and ensures that the responsibility of authentication remains with the user's institution. JISC, after much study and exploration, chose this access management solution, in part as it addressed the requirements that have been clearly defined since 2000. There is no doubt, however, that the move to Shibboleth over the next two years by UK further and higher education will pose many challenges and will require institutions to make some choices and decisions JISC (2006h).

## **2.6 Policy Issues**

In addition to technical developments, there are policy issues that arise from any implementation of an access management system, such as privacy, accountability (in relation to resolving abuse etc.), and the collection of management data. Lynch (1998b) makes an important observation when he wrote:

Libraries must decide whether to address these issues through legal means (that is, by negotiating contractual obligations on the resource supplier as part of the license agreement), through technical means (for example, by making it impossible to collect personal data), or by a combination of the two.

It is evident, throughout the discussion of access management systems, that greater management data has usually been achieved at the expense of the users' privacy. This is a tension that is not always considered during the discussions regarding access management, although the architecture behind Shibboleth does begin to address this area.

## **2.7 Summary and Areas for Further Research**

It is clear from the literature that the library and information community, particularly in the UK, will witness considerable change with regard to access management during the next few years. With such a period of change comes an opportunity to ensure that any access management solutions are critically assessed in line with a considered set of criteria.

The 'White Paper' by Lynch (1998a) has been correctly described as the 'departure point for most subsequent discussions of access management' (Robiette, 2000). In the seminal paper Lynch outlined a framework of seven criteria for the analysis and evaluation of proposed solutions to the access management problem. Despite the widespread adoption of both his terminology and definitions, the literature does not bear witness to the application of his criteria in quite the same manner. With UK higher education moving to the new Shibboleth solution over the next two years, and with many other authentication and authorisation systems in development (see Liberty Alliance (2006) and Windows CardSpace (Microsoft, 2006)), perhaps the criteria applied by Lynch should be applied to the current Athens and proposed Shibboleth access management systems. This process would ascertain whether the Shibboleth approach does indeed offer more benefits than the Athens solutions currently in widespread use. The evaluation would also present an opportunity to test the rigidity and applicability of the seven criteria and suggest improvements if needed. Any assessment would also need to engage with the tension of the policy issues, as identified earlier.

### **3. Methodology**

The purpose of this chapter is twofold. It aims to outline the definition of the mixed methodological approach and address the challenges that this approach presented. Secondly, the chapter outlines the design of the methodological approach that was employed in this study and to assess the implications, advantages and disadvantages of the chosen approach.

#### **3.1 Methodological Approach**

The access management systems under evaluation vary in nature in several significant areas. Some (AthensDA and Shibboleth solutions) utilise existing institutional usernames and passwords, whilst others (Classic and Personal Athens) involve the issuing of new credentials. In addition, Eduserv Athens is a production access management system, whilst the Shibboleth solutions are still predominantly under development. Furthermore, it is important to note that Shibboleth implementations will inevitably vary from institution to institution, given its nature as middleware rather than as a complete access management system.

In light of this varied research 'landscape', the only means with which to reflect, and engage, with the systems in question was to adopt a multi-method or blended approach, involving a mixture of methodological tools. In the case of Eduserv Athens a quantitative approach to data acquisition was appropriate, given that the majority, if not all, of the potential survey respondents would have had sufficient experience of the system and its variants to provide informed assessments. However, solutions based on Shibboleth were not widespread in UK higher education and, furthermore, not all of the Shibboleth implementations related to the control of access to electronic resources. Whilst an attempt to gain quantitative data was appropriate, it was recognised that more data might be gained from a comparative evaluation by the researcher. In this sense the critique of Shibboleth solutions was based more on a qualitative than quantitative methodological approach.

The mixing of methodological approaches is not without controversy, although this is not the place to rehearse the mass of arguments. Traditionally it has been the case that 'it is unacceptable to construct research projects which mix quantitative and qualitative methods' (Burton, 2000b p. 298), although more recently the mixture of methodologies has become more acceptable. Indeed, the term 'triangulation' has been coined to refer to the process (Bryman, 1988 p. 131). It would be a mistake, however, to assume that the use of mixed methods would necessarily derive the same data or produce the same findings. As Bryman (1988 p. 134) notes, 'discrepancies may also prompt the researcher to probe certain issues in greater depth, which may lead to fruitful areas of inquiry in their own right'.

One of the issues, particularly for qualitative methods, is perspective. Whilst the relationship between the researcher and the subject in quantitative research is often distant, it is much closer in qualitative research. In that context, it is recognised that qualitative researchers are also subjects and not outside of the process as impartial observers. As such, the researcher has what one commentator has termed a perspectival, rather than an objective, view (Maykut & Morehouse, 1994 p. 19) – namely a view that is inclusive of differing perspectives, 'including but not limited to the researcher's perspective'. Within this view the understanding of the meaning or definition of words is crucial. In this study, the engagement with the analysis framework defined below carried a risk that, despite the researcher's experience, the criteria were not understood as the original author intended. However, it was hoped that a clear exposition of the framework, together with study of the few published attempts at using the analytical method, would mitigate some of the subjectivities of the researcher and, subsequently, permit the blended methodological approach to assist the study.

### 3.2 Evaluation Criteria

The **Literature Review** identified the importance of the 'White Paper' by Lynch (1998a) to access management discussions since its publication. As well as establishing some of the key terminology, the paper also proposed an analysis framework and evaluated the prevalent (and proposed) access management approaches at that time, namely IP source filtering, proxies, credentials, digital certificates and hybrid schemes based on differing combinations of these. For the purposes of this study the criteria used in that evaluation will be expounded.

In summary, Lynch (1998a pp. 4-11) defined the framework for analysis in seven parts:

*Feasibility and Deployability* – from a user's perspective a system should 'facilitate access, minimizing redundant authentication interactions and providing a single sign-on, user-friendly view of the array of available networked information resources'. From the perspective of the institution the system should be easy to deploy and manage, scalable and able to adapt to change in the user community. In addition, the system should also be robust and simple to support.

*Authentication Strength* – the system should be reasonably secure, with the resource provider being confident that credentials can't be forged easily, and all involved being confident that the credentials cannot be easily stolen. Lynch made an important point when he noted that authentication strength is a subjective question. He wrote that 'strength comes from the details of cryptographic algorithms and key lengths used; but part lies in overall system design and implementation and in the realities of user behaviour, and this can often be the source of the largest number of vulnerabilities' (1998a p. 6).

*Granularity and Extensibility* – there is a need for fine-grained access control, where, for example, an institution could limit access to a resource to members of a particular class. This is one of the most controversial criteria, as fine-grained access is not currently practised to any great degree and, furthermore, licence agreements from resource suppliers do not support this approach. However there are suggestions that this is under review by suppliers, despite the concern about the potential for ‘irrational license economics’ (Lynch, 1998a p. 7).

*Cross-Protocol Flexibility* – this concerns the applications protocols or platforms that might be used for accessing information, noting that some systems are designed to work only with specific protocols, such as HTTP (for the web). In this discussion the main area of concern is the user’s workstation, which usually utilises the World Wide Web or telnet to connect to resources.

*Privacy Considerations* – Lynch noted that an electronic resource supplier may know a lot about who is accessing their service and when. Whilst provision and use of this information may be controlled by licence agreements, it is ‘desirable that the amount of privacy at risk which needs to be controlled by contractual provision be minimized’ (Lynch 1998a p. 8). One means by which user privacy can be protected is to ensure that users remain anonymous, although there are four identified levels of ‘anonymity’ in this context:

1. Anonymous Access – repeat users cannot be identified;
2. Pseudonymous Access – repeat users can be identified but the identity of the user cannot be determined;
3. Pseudonymous Access with Demographic Identification – no actual identities are revealed, but demographic information is determined.
4. Identified Access – actual identities can be associated with sessions.

It is possible that users may be offered additional services in return for less privacy or even identified access.

*Accountability* – within a contractual agreement for electronic resource access there is an element of trust and respect, particularly in relation to protecting the rights of the supplier. So, it is incumbent upon institutions to educate their users about the licence conditions, and to work with the supplier to identify, investigate and end improper use. However, this ability is in tension with the concerns of privacy, although there are models by which users may not be identified to the supplier, but their own true identity is known by their institution.

*Collection of Management Data* – there are essentially two types of data that the licensing institutions may gather, usage by user and usage of resource.

Management data is important to the decision-making processes of licensing institutions, although the use of this data is not without controversy, particularly if individual use is tracked. Lynch (1998a p. 11) identified this as a major issue, noting the conflict between privacy and the desire for demographic or individual data.

Given the importance of the ‘White Paper’, and the neglect of these criteria in recent discussion, these seven aspects formed the basis of the evaluation undertaken in this study. The framework for analysis directly informed and shaped the questions asked in the survey and interviews, and acted as the template against which Eduserv Athens and Shibboleth solutions were evaluated.

As the framework for analysis was first identified and applied in 1998, it was also appropriate that the framework was itself subjected to a critical assessment. Therefore, following its application to a study of the Eduserv Athens and Shibboleth solutions, the framework was assessed to ensure its continued validity in the study of access management systems.



## **3.3 Research Design**

### **3.3.1 Range of Systems**

As has been indicated earlier, the subjects of this study were the access management systems currently in use in UK higher education, namely Eduserv Athens and its variants, and the recently proposed approach based on Shibboleth (JISC, 2006a). The study did not include an assessment of IP address filtering, proxies, individual credential sets, or certificate-based credentials, which were adequately evaluated elsewhere (Lynch, 1998a; Paschoud, 2004 p. 149-151; Sävilammi, 1998).

### **3.3.2 Perspective**

Each access management system was evaluated from the perspective of someone who would implement and administer such a system for an institution. This included institutional Athens administrators (or members of the institutional Athens team) and those technical specialists responsible for installing, developing and maintaining AthensDA and Shibboleth solutions. End users of the access management systems were not surveyed for two reasons:

1. some access managements systems are seemingly 'invisible' to the end user, particularly if the system is 'badged' with a localised service name (such as 'Electronic Library Login') or is based on an existing institutional credential set;
2. an end user would not experience the various aspects of an access management system, such as management data collection or deployment.

It was noted, however, that administrators and developers of access management solutions are also end users. This may therefore have been reflected in their responses to data collection, perhaps more so in responses where they were less confident of a response. This was a consideration during the data analysis.

The researcher is an Athens administrator and a technical developer, having experienced all the systems under evaluation, and thereby conformed to the required perspective when engaging in the (particularly qualitative) analysis.

### **3.3.3 Sample**

In order to satisfy the requirements of the perspective, outlined above, it was necessary to target those categories of professionals that were involved with access management systems as Athens administrators, or as technical developers. As the study also addressed one aspect of the UK educational sector, it was necessary to ensure, where at all possible, that the survey respondents, and interviewees, were from higher education.

A definition of 'higher education' was less than easy to identify, however. For this study, UK higher education was taken to refer to all those higher education institutions in England, Scotland, Wales and Northern Ireland that were funded by the various higher education funding bodies. Those funding bodies were as follows:

- Higher Education Funding Council (HEFCE) - England
- Scottish Higher Education Funding Council (SHEFCE)
- Higher Education Funding Council for Wales (HEFCW)
- Department for Employment and Learning, Northern Ireland

The funding bodies provided financial support to 165 institutions (counting the various Open University listings as one).

Of further interest was the number of institutions that used Eduserv Athens. At the time of the survey 206 institutions were registered as using Athens access management (Eduserv, 2006c). This suggested that many privately funded higher

education establishments also used Eduserv Athens – a factor that needed to be considered in the data collection.

### 3.3.4 Obtaining the Data

#### Timing

The aim of this dissertation was not only to evaluate the access management systems currently in use within higher education, but also to attempt an evaluation of the Shibboleth solution proposed by JISC as the replacement national service. As indicated in the **Literature Review**, approaches utilising Shibboleth for managing access to electronic resources have been piloted as part of the JISC Core Middleware Infrastructure Programme (JISC, 2004g). Whilst the programme is still ongoing at the time of writing, the majority of the projects in the first phase finished by June 2006 and most of the final have been submitted to JISC (although not all reports were publicly available). In light of this timing, it was important that the quantitative and qualitative analysis was undertaken after May 2006 for the following reasons:

- the majority of the final reports will be available for analysis, if not publicly then probably to the programme members (such as the researcher);
- the projects' completion meant that more library staff, particularly institutional Athens administrators, *may* have had the opportunity to take part in a Shibboleth.

This study recognised, however, that exposure to a Shibboleth access management solution was limited and this may have had a detrimental impact on the level of evaluative data received for that particular method.

In light of data availability, particularly in relation to Shibboleth, this study gathered a significant proportion of the quantitative and qualitative data since June 2006.

The survey, the main method by which quantitative data was acquired, was open to respondents in August for 12 days.

## **Survey**

It was decided to obtain a significant proportion of the evaluative data via a survey. An online survey facility (SurveyMonkey.com) was preferred to a manual, printed survey for a number of reasons, primarily: ease of access, delivery speed, turnaround time, appropriateness to the audience (online professionals), and improved response rate. However, it was recognised that online surveys have some disadvantages. One common issue is that online surveys can be unrepresentative of the population, with their reliance on Internet access. Given the nature and topic of this study and the target sample, however, this was not a significant concern. Burton (2000a p. 329) identified a further issue regarding spontaneous answers, with respondents often being able to see all of the questions, so different answers could not be treated as independent. This was mitigated to an extent in the online survey by the division of the questions into sections, often with only one evaluative question per page, allied with a careful navigational structure. In addition, the respondents were not permitted to browse ahead in the survey without first completing the questions on the current page. One concern, shared with printed surveys remained, however - it was difficult to be sure that the intended sample actually answered the survey, although measures were taken in this research to reduce this possibility.

The questions and structure of the survey were determined by the analysis framework outlined by Lynch in his 'White Paper' (1998a pp. 4-11). It was important to follow this approach, given that the continued suitability and robustness of the evaluative criteria, as presented in that paper, were being assessed, as well as the actual systems. This approach facilitated easier comparison of the requirements and efficacy of the systems. The framework of analysis was in narrative form, with extensive discussion of the seven areas. For the purposes of the survey it was necessary to identify the key elements of each of

those seven criteria and convey them in clear, concise questions and survey constructs.

Following a review of best practice with regards to online survey design, an approach influenced by that taken by the JISC Monitoring Unit (JMU) (2006a) was adopted. The JMU had recently carried out the Annual Survey of Network Content Services 2005/2006 (JISC Monitoring Unit, 2006b), which included questions regarding the Athens authentication service. Elements of the JMU survey briefly touched on the subjects of this study, and targeted similar samples, so utilising a familiar approach, it was hoped, would elicit more responses than might otherwise have been the case.

A pilot of the survey was undertaken, involving several information professionals, some under observation. The pilot enabled an estimation of how long the data collection would take (approximately ten minutes) and provided feedback on the style and substance of the questions. It also provided an opportunity to check the 'flow' of the overall survey design. As a result amendments were made to some wording and the general flow of the survey. Following the amendments, the survey was trialled again, before eventual release.

The survey consisted of thirteen 'screens'. Following an introductory screen, the survey commenced with two open questions relating to the role and departmental allegiance of the respondent. Both questions had pre-defined answers together with an 'others' category where the respondent could enter an alternative answer.

Four approaches to access management were then assessed using closed questions, with Eduserv Athens being evaluated according to its three modes – Access Accounts, Personal Accounts, AthensDA - and solutions based on Shibboleth. In each case the respondent was asked if their institution had used, or currently used, that access management approach. If the answer was negative

the survey directed the respondent to the next approach, and so on, until the respondent arrived at the closing two screens. If the answer was positive, the respondent was invited to evaluate that system.

Each of the four systems was assessed against the same list of thirteen criteria. These were developed from the original seven aspects of the analysis framework, with some of the wider areas being explored by more than one evaluative element. The questions were predominantly closed in nature, with respondents being asked to rate the systems against the thirteen criteria using a rating scale of 1 to 5, where 5 equalled excellent, 4 good, 3 satisfactory, 2 mediocre, 1 poor. No 'opt-out' or 'not known' was provided – this was a deliberate decision made in recognition that the target sample would be in a position to answer, given their expertise. However it was recognised that this might prompt a few respondents to rate an element as satisfactory when perhaps they might have used an opt-out option.

All respondents were directed to the final two screens. The penultimate screen involved the ranking of eleven factors (based on the thirteen criteria elements used in the previous questions) based on their importance to the respondent, 1 being the most important and 11 the least. All eleven factors had to be assigned a ranking with one factor per rank, in a closed question format. No joint ranking was permitted. A second question asked the respondent to rate the four access management approaches in terms of providing what they needed to control access to their institution's electronic resources, using a numeric rating scale, as before, from 5 being excellent, to 1 being poor. These two questions were developed to gain an insight into the priorities in access management as seen by the sample. This provided a background against which the results of the survey could be further assessed. The full list of survey questions, and structure are provided in **Appendix A**.

The survey was targeted at the sample with participation calls on five electronic mail distribution lists, all hosted by JISCMail, the national academic mailing list

service – athens, athensda, jisc-shibboleth, jisc-core-middleware and lis-link. An example of the e-mail posted can be found in **Appendix B**. Whilst the first four lists were populated by those directly involved in Athens and Shibboleth, the latter was a general list for the wider library community. The use of these five lists had clearly identifiable advantages and disadvantages. The advantages were:

- quick and easy distribution of the call;
- membership of the lists was voluntary, so people join them usually because of their interest or involvement in the subject area of the list;
- messages, when received by those to whom the message does not apply, can be easily forward to the correct recipient.

The disadvantages were:

- unable to guarantee that all of the required sample receive the message (this is also true of printed surveys);
- those who do not fit the sample profile might receive and act on the message.

The e-mail messages introduced the survey and its purpose, and assured potential respondents of anonymity for both them and their institution in the research. As an incentive, to encourage responses at a time of the year when responses are traditionally lower, the call also included details of a draw for a gift certificate which was optional to all those who took part (the entry form was at the end of the survey, thus ensuring completion first).

## **Interviews**

Whilst the main source of data for this research was the survey, which provided predominantly quantitative data, it was decided to interview two people, both survey respondents, to explore further their understanding of the issues. The

mixing of methodologies, as has been described earlier, is an area of considerable debate. However, the use of interviews, a qualitative approach, in this context can assist the quantitative research. Among some of the benefits that Burton (2000b p. 298) identified, the qualitative approach can be a 'mechanism for validating survey data' and can offer 'case study illustrations'. It was also recognised that this triangulation can enable 'researchers to strengthen the validity of their findings if both are able to provide mutual confirmation' (Bryman, 1993), although this result is not necessarily guaranteed.

In this context, the two interviews were used to assist in the validation of the survey data and provide some additional material that could be used in the wider analysis. To ensure full coverage of the survey subjects, the two interviewees were chosen with care. One was the Athens administrator for a higher education institution, the other a technical developer on a Shibboleth implementation project. The interview schedule was designed to reflect, to some extent, the same framework of analysis used in the survey, although some additional material was added. Whilst the interviews followed a schedule, the questions were sufficiently open to permit further exploration of issues as required. The interview schedule is included as **Appendix C**.

### **Comparative Analysis**

One of the few direct engagements with the 'White Paper' analysis framework (Lynch, 1998a) was by Sävilammi (1998). Sävilammi compared some authentication-based models by entering their distinctive features in a comparative table (1998 section 4.1.5). In this table the systems were assessed against the seven areas defined by Lynch, with an eighth entry ('more') for additional information. The presence of this eighth 'undefined' entry in the table, and the rearrangement of some of the criteria divisions, is significant – did this indicate that the framework was insufficient as a comparison tool or did it mean that Sävilammi did not fully understand the meaning of the seven criteria and was therefore unable to correctly categorise the features?



Whilst the survey produced a wealth of quantitative data, it was necessary and appropriate that the table comparison be repeated, albeit this time for the four methods under assessment in this study. In order to ensure that the researcher was not unduly influenced by the quantitative data, this analysis was performed prior to the compilation and analysis of the survey data. With extensive experience of all four methods, the researcher was in an ideal position to carry out this qualitative comparison. However, as Säviammi may possibly have shown, this method was not without its risks.

### **3.4 Presenting the Results**

Having acquired the data from the survey, it was possible to enter the information into Microsoft Office to facilitate the use of descriptive statistical techniques to present the research results. This was then subjected to statistical analysis. Furthermore, the data from the researcher's qualitative analysis of the systems was entered into tables in Microsoft Word. Additional material from the interviews was used in the qualitative analysis and overall discussion. The analysis enabled the researcher to reach conclusions which addressed the overall objectives of the study. The results of the analysis are presented and discussed in the following chapters.

## 4. Research Findings

This chapter presents the findings of the online survey and the interviews, described in the previous chapter, and raises issues for later discussion.

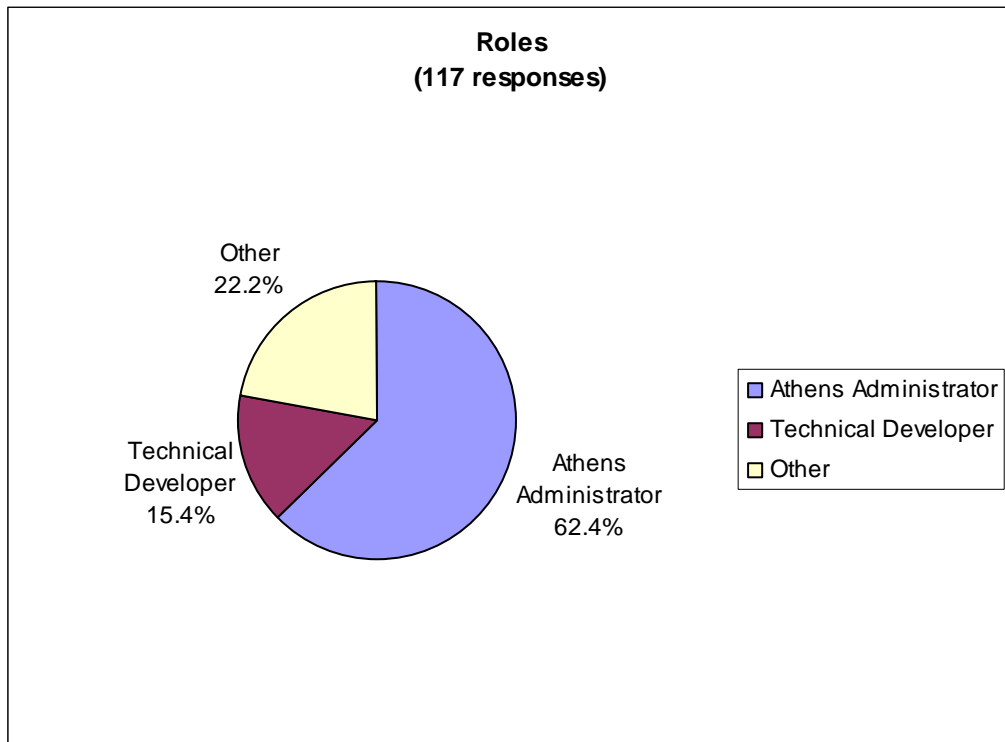
### 4.1 The Sample

The online survey targeted those information professionals in UK higher education who were involved with access management systems, as Athens administrators or as technical developers. Five JISC Mail e-mail distribution lists were chosen as the means by which to place a call for participation.

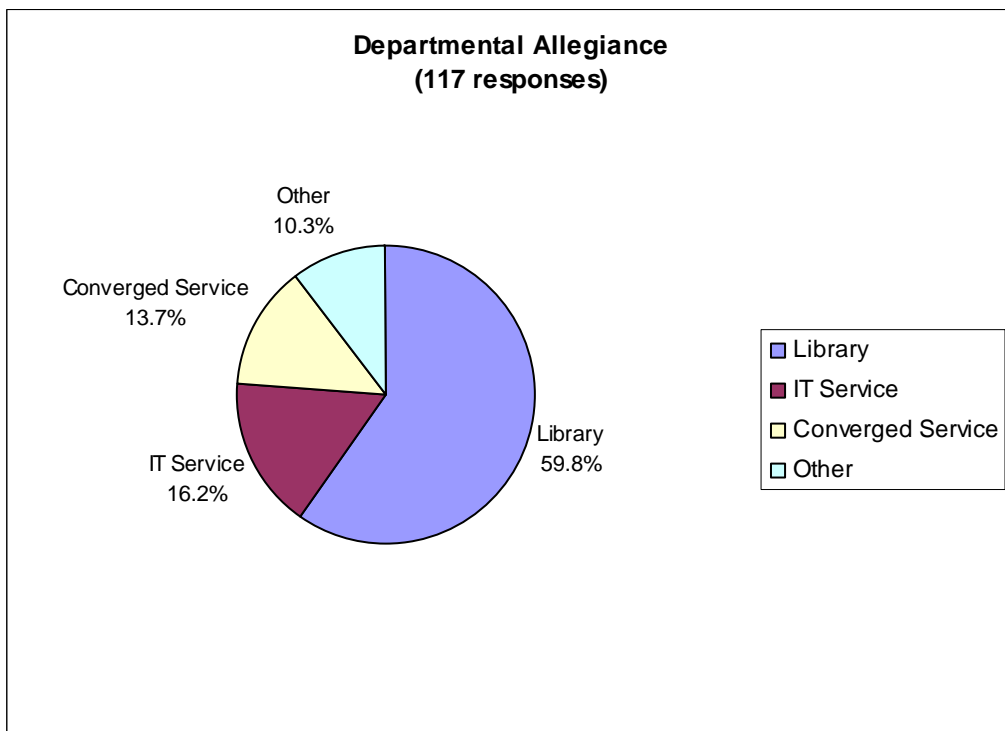
From the calls 117 people completed the survey. The roles performed by those respondents are detailed in **Figure 1**. The majority of respondents, 63%, were Athens administrators, although 26 used the open question to define their role (see **Appendix D**). Responses included manager, e-resources librarian, systems librarian, and project manager, among others. Two respondents defined themselves as both Athens administrators AND technical developers. Some comparisons are made in the following discussions about the differences in responses between these groups, although the relatively small sample of technical developers inevitably has some bearing on the value of this exercise.

**Figure 2** shows the departmental allegiance of the respondents. Almost 60% of the 117 respondents defined their department as a Library Service. Of the remainder, 12 respondents defined their own allegiance, with responses including archive, marketing and academic support (see **Appendix D**).

**Figure 1 Survey Respondents: Role**



**Figure 2 Survey Respondents: Departmental Allegiance**



Respondents were asked to identify which of the four approaches to access management they had used (Athens Access Account, Athens Personal Account, AthensDA and Shibboleth) and the evaluation screens were then presented on the basis of that choice. Consequently not all respondents completed evaluations for all the systems, as **Table 1** shows. The figures show that respondents are most familiar with the credential-based approaches of Eduserv Athens. It should also be noted that respondents may have evaluated more than one approach, due either to parallel use or previous experience. The low response figure for Shibboleth is not surprising, given that the formal announcement by JISC (2006a) to adopt Shibboleth was made only this year and exposure to its implementation is limited to those involved in the various JISC Core Middleware Programme projects. This low response will inevitably have some bearing on the interpretation of the results.

---

**Table 1      Respondents per Access Management Approach**

---

<b>Access Management Approach</b>	<b>% of total sample</b>	<b>Response Totals</b>
Athens – Access Accounts	53.0%	62
Athens – Personal Accounts	62.4%	73
Athens – AthensDA	27.4%	32
Shibboleth	7.7%	9

## **4.2 Comparative Evaluation**

The main element of the survey involved the assessment of each of the four access management approaches according to thirteen factors, which correlated to the seven criteria used in the ‘White Paper’ analysis framework (Lynch, 1998a pp. 4-11). A numeric scale was used where 5 = excellent, 4 = good, 3 = satisfactory, 2 = mediocre and 1 = poor.

The evaluation results are grouped, below, according to those seven criteria and the findings for the access management systems are presented alongside each other. The thirteen tables on which the following discussion is based can be found in **Appendix E**. The tables are numbered **E1** to **E13** and they are identified using this nomenclature throughout the ensuing discussion. The red entries in those tables indicate the predominant response.

In addition, relevant comments from the two interviewees are noted in the accompanying discussion. The Athens administrator is identified as **Interviewee A** and the Shibboleth developer is identified as **Interviewee S**.

#### **4.2.1 Feasibility & Deployability**

This aspect of the analysis framework was reflected in the provision of three factors for the respondents to rate (see **Tables E1, E2** and **E3**):

- ease of implementation
- ease of maintenance
- suitability for distance users

The last factor related to the comment by Lynch (1998a p. 5) that any solution ‘must be able to recognise the need for a user community member to access a resource... independent of his or her physical location’.

In terms of implementation, all four approaches were predominantly rated ‘good’ (47% for both Athens Classic and Personal Accounts, 41% for AthensDA, 33% for Shibboleth). Negative ratings were few in number, with only Shibboleth receiving any significant ratings, 22% being ‘poor’. There was greater variation in the responses to ease of maintenance, with Athens Classic and Athens Personal

Accounts both receiving more negative ratings (15% and 21% respectively). The ease of maintenance was rated highest for AthensDA (38% 'excellent', 28% 'good' and 31% 'satisfactory'), with Shibboleth predominantly rated 'satisfactory' or better. Overall, ease of maintenance seems to be rated higher for those systems that rely on existing institutional logins.

The systems' suitability for distance users (i.e. those not using the institution's IP address range) drew a more marked difference in responses. Athens Access Accounts were rated the least satisfactory, with a 'poor' rating of 31% and a 'mediocre' rating of 13%. Ratings were more positive for Athens Personal Accounts and AthensDA, with the majority of ratings 'good' or 'excellent' (79% for Personal Accounts and 88% for AthensDA overall). Shibboleth did not receive any negative ratings, with the predominant rating being 'good' at 33%.

Interviewee A reported that AthensDA, whilst technically a challenge to implement, was a lot more effective than Personal Accounts, which required more account maintenance work. They noted, however, that the locus of responsibility for most of the maintenance had shifted to IT Services with AthensDA. Interviewee S emphasised the steep learning curve for Shibboleth and the wide range of technical skills involved. The importance of an identity management system as a pre-requisite for a successful Shibboleth implementation was also stressed.

#### **4.2.2 Authentication Strength**

One factor was assessed (see **Table E4**) for this section:

- security

Of note in these results was the confidence in the security of those systems that involved the direct use of existing institutional accounts, as with AthensDA and Shibboleth. In both these cases no negative rating was received, with the majority

rating at 'excellent' or 'good' (94% for AthensDA and 100% for Shibboleth). However, whilst the confidence in Athens Access and Personal Accounts was rated 'good' to 'satisfactory', both modes received some negative ratings. More respondents (24%) gave a negative rating for the shared account credentials, as used with Access Accounts, than the personalised credentials of Personal Accounts (13%).

When comparing the differences in responses between Athens administrators and Technical Developers, it was interesting to note that the latter were much more negative about the security of Athens Access Accounts (40%, compared to 19% for Athens administrators).

Interviewee A noted the ease by which Personal Athens Accounts could be passed to other users and identified the issue of trust as key to the success of the approach. They also noted the greater impact and risk to users if the credentials used with AthensDA were compromised, given their use with other institutional services like e-mail. Interviewee S described Shibboleth as being 'designed with security at its heart', although they noted that the security of the institutional Single Sign-On (SSO) was integral to the system too.

### **4.2.3 Granularity & Extensibility**

This aspect was reflected in the provision of four factors (see **Tables E5, E6, E7** and **E8**):

- ability to include other sites within the institution
- control of access to resources by class or group level
- flexibility to cope with more users or a changed institutional structure
- suitability for users with affiliations to multiple institutions

Dealing with the issue of extensibility, both AthensDA and Shibboleth were rated higher with regard to the inclusion of other sites within an institution, with only one negative respondent between them. Again, the worse performer was the Athens Classic Account, with 40% rating it 'satisfactory' and 24% rating it negatively. Personal Athens Accounts were highly rated, with 22% 'excellent' and 40% 'good'.

A similar story emerged in the responses to the ability of the system to cope with more users and/or a changed institutional structure. Again Athens Access Accounts fared the worst, although the majority of respondents were positive (40% 'satisfactory', 31% 'good' and 8% 'excellent'). The ratings for Personal Athens Accounts were marginally better, with the predominant rating being 'good' at 41%. The systems based on institutional logins, however, received higher approval, with 50% rating AthensDA 'good' and 25% 'excellent' (with only one respondent returning a negative rating) and 56% rating Shibboleth 'good' and 22% 'excellent' (again with one negative rating).

The responses relating to suitability for users with affiliations to multiple institutions deviated from the pattern shown above, with the predominant response being 'satisfactory' across all four systems (Access Accounts 43%; Personal Accounts 32%; AthensDA 32%; Shibboleth 44%). Such a uniform response may suggest that other factors influenced responses, possibly owing to uncertainty or lack of experience of the topic.

On the issue of granularity, namely authorising resource access to class or group level, the overwhelming rating for all systems was 'good', with all ratings 42% to 48%, except for Shibboleth at 67%. There were few negative ratings – although, against the dominant pattern, Personal Athens Accounts received the most (17%, compared to 11% for Access Accounts and 9% for AthensDA).



During the interviews, it was suggested that Shibboleth permitted a greater level of granularity in relation to access control. Interviewee S, however, warned that the methods used within Shibboleth for this level of granularity were administratively demanding, although solutions were in development to address this. Interviewee A talked of the methods within Athens to define levels of access, although, interestingly, they felt that it was easier to administer with Personal Athens Accounts.

#### **4.2.4 Cross-Protocol Flexibility**

This aspect was reflected in the provision of one factor to be rated (see **Table E9**):

- effectiveness for a wide range of network protocols

The predominant rating across all four approaches was 'satisfactory', with few negative responses. Furthermore, there were few, if any, noteworthy differences in the responses of the two main roles. The general response to this factor may indicate a lack of understanding or knowledge about the issue and warrants further exploration.

#### **4.2.5 Privacy Considerations**

One factor represented this aspect of the analysis framework (see **Table E10**):

- protection of user privacy

Once again there was a distinct difference in the ratings between the credential-based approaches (Athens Access and Personal Accounts) and those reliant on existing institutional accounts. AthensDA and Shibboleth received no negative ratings, with both having received a majority of 'excellent' (AthensDA 41%, Shibboleth 56%) and 'good' (AthensDA 41%, Shibboleth 44%) ratings. However,

very few negative ratings were received for the other two approaches (8% - 9% each). Both Access Accounts and Personal Accounts were rated as 'good' (47%-49% each) to 'satisfactory' (30%-34% each). There was little difference in the ratings of Athens administrators and technical developers. It is clear that privacy was rated higher where existing institutional login credentials are used.

Interviewee A noted that the privacy levels of Personal Athens Accounts depended, in part, on the username chosen (as they can be selected by the user, depending on implementation). Personal Accounts were also not 'encoded' in the manner of AthensDA accounts, which were described as more effective in maintaining privacy. With regards to Shibboleth, Interviewee S noted the compromises often involved in creating virtual identities for users, particularly when they required personalisation services at the resource provider, and recognised the value of pseudonymous identities to provide such facilities whilst maintaining a level of privacy.

#### **4.2.6 Accountability**

This aspect was reflected in the provision of one factor in the survey (see **Table E11**):

- individual user accountability

Athens Access Accounts were rated the worst in the provision of individual user accountability, reflecting the shared nature of the account type. Whilst overall it was rated as 'good' (34%) to 'satisfactory' (26%), some 21 respondents (34%) rated it negatively. Aside from two respondents rating AthensDA 'mediocre', the remaining three approaches were rated 'satisfactory' or higher, with AthensDA and Shibboleth receiving higher marks. Again, the approaches utilising existing institutional login credentials were rated higher.

In a comparison of the responses from the two main roles, technical developers consistently rated each system consistently less, only 'satisfactory' in the case of Athens Access and Personal Accounts (compared to 'good' by Athens administrators) and 'good' (50%) for AthensDA, compared to 'excellent' (44%) from Athens administrators.

Interviewee A felt more able to track user behaviour with Athens Personal Accounts, even though AthensDA permitted the institution to identify online behaviour easily. This was not so much because of the technology, but rather the locus of the work involved, with IT Services more able to identify users owing to their responsibility for the local LDAP directory from which AthensDA identities are derived. Interviewee S commented that the privacy of Shibboleth users depended on the underlying installation and the logging options defined within it. However, it was remarked that there were, currently, no useful tools to digest that sort of information.

#### **4.2.7 Collection of Management Data**

This aspect of the analysis framework was reflected in the provision of two factors (see **Tables E12** and **E13**):

- collection of management (usage) data at user level
- collection of management (usage) data at resource level

The collection of management data is performed at user and resource levels and it was important to make this distinction by asking two separate questions. This approach would highlight any fundamental differences between, and also within, each approach to access management.

The responses suggested that there was a difference in the abilities of Shibboleth to collect management data, with data for resources usage predominantly rated at 'mediocre' (44%), whilst that for users was predominantly rated 'good' (44%). Whilst the small sample means that firm conclusions can not be drawn, this division does reflect the fact that Shibboleth is middleware and NOT a fully featured access management system like Eduserv Athens. As such, its ability to collection management data is much less defined.

The other distinction that was highlighted related to the abilities of Athens Access Accounts. More responses rated collection of user data to be 'mediocre' or 'poor' (37%) compared to the same for resources usage (14%), though both types were rated predominantly 'satisfactory'.

Both Athens Personal Accounts and AthensDA were both more positively rated across both collection data types, with Personal Accounts predominantly rated 'good' for both (53% for user and 55% for resource usage), whilst AthensDA was predominantly rated 'satisfactory' for both (50% for user and 47% for resource usage).

Interviewee S remarked that Shibboleth was 'too young a product' to have a management suite and said that facilities for management data collection would be dependent on the nature of the local implementations. More importantly the interviewee pointed out that the technical protocols on which Shibboleth is based do not specify a management system. Interviewee A was more positive about the data collection facilities of Eduserv Athens and the administrators' interface.

#### **4.2.8 Overall Assessment**

Against the same ranking scale as outlined in **Section 4.2**, the respondents were asked to rate each of the four access management approaches under review in terms of those systems providing what they required to control access to their

institution’s electronic resources. Unlike previous rating questions, respondents were given a ‘not applicable’ option. The results can be seen in **Table 2**, below.

The ratings clearly show that the shared account approach of Athens Access Accounts was the least rated, with 30% of respondents rating it ‘satisfactory’, alongside 29% rating the approach ‘mediocre’ or worse. Only 17% of respondents did not offer a rating.

**Table 2 Overall Rating of all Four Approaches to Access Management**

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>n/a</b>
<b>Athens: Access Accounts</b>	9% (6)	16% (11)	30% (21)	20% (14)	9% (6)	17% (12)
<b>Athens: Personal Accounts</b>	17% (12)	37% (26)	29% (20)	9% (6)	1% (1)	7% (5)
<b>Athens: AthensDA</b>	19% (13)	26% (18)	10% (7)	1% (1)	0% (0)	44% (31)
<b>Shibboleth</b>	20% (14)	17% (12)	9% (6)	0% (0)	1% (1)	53% (37)

Athens Personal Accounts were rated ‘satisfactory’ (29%) to ‘good’ (37%), with a further 17% at ‘excellent’. Negative responses were low (10% overall) and non-respondents numbered only 7%.


The response level for AthensDA dropped, with 44% selecting ‘not applicable’. Despite this, all bar one respondent rated AthensDA at least ‘satisfactory’, with the majority selecting ‘good’ (26%) or ‘excellent’ (19%).

Shibboleth was the most positively rated, although a much higher percentage (53%) of the respondents did not take part. This was understandable, given the limited exposure that many of the respondents have had to Shibboleth.

### 4.3 Priorities in an Access Management System

The final question in the survey sought to determine the respondents' priorities in an access management system by presenting them with 11 factors (approximately equating to the 13 criteria rated in the previous questions). These factors had to be ranked in order of importance to the respondent, 1 being the most important and 11 being the least. All factors had to be ranked, with only one factor to each rank, i.e. no joint rankings were permitted. The results can be seen in **Table 3**. The full statistics are in **Appendix F**.

**Table 3 Ranking of Factors / Facility in Order of Importance**

Rank	Factor / Facility
<p style="text-align: center;"><b>Most Important</b></p>  <p style="text-align: center;"><b>Least Important</b></p>	Ease of Implementation
	Facilities for Distance Learners
	Ease of Maintenance
	Strong Security
	Flexibility to Cope with Changes and Additions
	Cross Platform Functionality
	User Privacy
	Individual User Accountability
	Collection of Management Data
	Fine Granularity
	Facilities for Users with Multiple Institution Affiliations

Interestingly, some of the most challenging aspects of access management were ranked the least important, such as facilities for users affiliated to multiple institutions and finer levels of granularity.

Ease of implementation and maintenance were ranked highly, together with facilities for distance learners. Cross platform functionality, a factor that can be interpreted in different ways, featured more so than the privacy, and accountability, of users. This is interesting, particularly in relation to privacy, given that Shibboleth has been built on the basis of high user privacy.

#### **4.4 Summary**

It is evident from the survey results, summarised above, that, in some areas, there is a distinct division between those systems based on existing institutional accounts (AthensDA and Shibboleth) and those where additional account details are required (Athens Access and Personal Accounts).

There is also some evidence to suggest that some of the facilities or factors being ranked may not have been fully understood or, owing to the respondent's perspective, fully appreciated within the wider context of access management. These issues, and more, are explored in the next chapter.

## 5. Discussion and Analysis

This chapter discusses the research findings with particular reference to the aims and objectives as stated in the **Introduction**.

### 5.1 Access Management Systems

It was essential that the current and proposed access management systems in U.K. higher education were identified. The **Literature Review** duly ascertained Eduserv Athens and Shibboleth as, respectively, the current and proposed systems. Furthermore, Athens was shown to offer access management functionality in several forms, as noted by Norris (2004, p. 278). Following the identification of a framework of analysis (Lynch, 1998a pp. 4-11), the four systems were evaluated using various methodological tools and the significant outcomes are outlined below.

#### 5.1.1 Athens Access Accounts

Access Accounts were the oldest of the systems reviewed and, functionally, the most limited. The shared account approach, and their restriction, often, to institutional IP ranges, has inevitably led to limitations, as indicated by the survey results. As one of the two systems reliant on the issuing of additional account details, the rating of Access Accounts was consistently lower than those that relied on existing institutional logins.

Access Accounts, whilst perhaps the easiest to deploy, do not address the needs of distance users. Nor do they utilise an SSO approach or authenticate within the local domain. Inevitably, their shared nature presents a challenge to system security, a fact recognised by the survey respondents. This arises not from the technology but rather the users, who are the largest threat to the integrity and security of Access Accounts.



In terms of extensibility, Access Accounts are capable of dealing with changes in the institutional structure and can accommodate other sites by virtue of the shared account. The granularity of Access Accounts is dependent on their deployment, however. Whilst it was rated moderately, some granular access control is possible, although rarely beyond departmental level. Consequently, across this aspect of the analysis framework, Access Accounts were generally recognised to have significant functionality, despite some negative ratings.

The privacy of the shared Access Accounts was, not surprisingly, rated positively, given their lack of assignment to any one individual. However, the tension between privacy and accountability is highlighted by the negative responses returned for the latter aspect. As individuals are not specifically linked to the account, the options for identifying users in the event of misuse are limited. This tension is further observed in the survey results in relation to management data – whilst the shared account permits collection of usage data for resources, the lack of identifiable users limits the system's capability to collect data by users and subsequently is unable to provide any demographic statistics.

### **5.1.2 Athens Personal Accounts**

Personal Accounts, like Access Accounts, involve the issuing of an additional credential set. However, these accounts are unique to each individual and are not shared. This inevitably increases functionality, a fact reflected in the survey results, with a generally more positive reception across all aspects. However, some factors need further exploration.

Whilst suitability for distance users was well rated, this masked a secondary issue. Whilst personalised accounts, not restricted by location, are ideal for distance users, the mode of the initial account delivery necessarily has some impact on the overall assessment – for instance, are the accounts automatically created and delivered on registration, created via self-registration, or created on request? Self-

registration is often only permitted within the institutional IP range, thus presenting a barrier to distance users.

Whilst they received less negative feedback regarding security than Access Accounts, Personal Accounts did, nonetheless, receive some. This may be a reflection of their 'portable' nature, a point also highlighted by Interviewee A. With little 'risk' to the user if their account is shared or compromised, these accounts are sometimes passed to others, thus potentially compromising licensing conditions.

The aspects of the analysis framework where identification is integral drew some interesting results that are explained, in part, by the individual allocation of Personal Accounts to users. However, this is by no means the fully story. The overall assessment is also determined by the very nature of the username assigned to each user. If this is set to have some reflection of their real identity, then privacy is compromised. Conversely, if the username bears no relation to the user's real identity, then privacy is improved. Again the responses in the survey have masked a secondary issue. Accountability is inevitably rated highly, as the user's institution is the issuing authority and will have user records. The same is also true of the collection of management data – of both types.

### **5.1.3 AthensDA**

AthensDA, one of the two methods based on existing institutional logins (where authentication is performed by the user's institution), was consistently rated higher across all sections by respondents. A significant factor in the assessment of AthensDA is its intrinsic link to other services and systems. Unlike Personal Accounts, the credential set used in an AthensDA transaction is also the credential set for many other localised services, such as e-mail. Access to electronic resources is granted following authentication by a third party, thus necessarily requiring a significant level of trust between the authenticating (user's) institution, Eduserv Athens and suppliers of resources. This element of local authentication

addresses one of the central commitments of JISC, as first outlined six years ago (Robiette, 2000).

With regards to privacy, the AthensDA transactional process involves the creation of a persistent but pseudonymous identity, from the local authentication, via an algorithm. It is this identity, often a long series of seemingly random numbers and letters, which is passed to the resource. Therefore, whilst a real identity is not conveyed to the resource supplier, the function of accountability remains, as the algorithm is constant. At the institutional level, it would be possible to reverse the process to derive a real identity from the AthensDA pseudonym, although this process would not be straightforward. This explains the high survey ratings achieved in relation to privacy, accountability and, to some extent, management data collection.

The link with institutional logins means that AthensDA is well suited to the needs of distance users and this was reflected in the survey results. Whilst there is still the issue of delivering the initial institutional login to users, this process is often better accommodated at the beginning of a users' relationship with the institution. This leads to an important issue regarding this assessment of AthensDA.

A considerable part of the AthensDA process, particularly its implementation and maintenance, is not in the domain of the Athens administrator (unlike Access or Personal accounts) but rather the domain of technical developers, often in other departments. This means that the Athens administrators' experiences of some elements of the analysis framework for AthensDA are somewhat limited. For example, an Athens administrator may rate the ease of maintenance for AthensDA quite highly, based on the fact that they do not have to do anything to ensure that users are registered – the process may well be automated following extensive work by a technical developer elsewhere. As discussed in the **Methodology Chapter**, the issue of perspective is significant here. To what extent were the ratings for ease of implementation and ease of maintenance well informed, given

the predominance of Athens administrators (63%) among the respondents? Unfortunately the sample for technical developers was too small to make any statistically meaningful comparisons.

#### **5.1.4 Shibboleth**

Shibboleth is another method based on existing institutional logins, where authentication is performed by the user's own institution, as with AthensDA. However, unlike AthensDA, Shibboleth is not a complete access management system; it is middleware, utilising the SAML security protocol, enabling communication between differing systems. This differing nature, together with the small sample of respondents (9, evenly distributed across roles) who rated Shibboleth, made a direct evaluative comparison with the other systems more difficult. Indeed the small sample did not permit the formation of confident statistical outcomes. However, some patterns can be drawn, albeit tentatively, from the responses.

An indication of the technical challenges associated with Shibboleth implementation was suggested by the negative survey ratings and confirmed by interview – one of the few aspects where the rating of Shibboleth was significantly different to that of the other systems. The nature of Shibboleth was further highlighted by the contrast in responses to data collection, where the collection of resource usage was negatively rated – recognising the lack of any integral management data collection components.

The evaluation of Shibboleth in this study was fraught with problems. Notwithstanding the small sample, and limited exposure of respondents to the technology, Shibboleth dramatically differs in some key areas from those systems provided by Eduserv Athens. As JISC (2004f) agreed, Shibboleth can only be compared on a technical level – the survey, and by association the analysis framework, attempted much more.

### **5.1.5 Overview**

The most significant outcome of the evaluation was that the systems which utilised existing institutional account credentials were rated higher than those that required additional login details. Furthermore, the shared account nature of the Athens Access Accounts clearly did not positively address some of the criteria in the analysis framework. A tabular summary of the strengths and weaknesses of all four systems can be viewed in **Appendix G**.

There is no doubt that Single Sign-On (SSO) functionality contributes significantly to the success of AthensDA and Shibboleth. It is obvious that SSO makes life simpler for the users and, to some extent, those who administer such access management systems. However, the advantages bring new issues – the increased reliance on local technical developers (more so with Shibboleth) and increased risk to users (who have more to lose if their account is compromised or shared).

Despite the small sample, the qualitative and quantitative study of Shibboleth confirms that the technology does address the requirements of JISC for a national access management system, something that cannot be claimed by the other systems under review.

## **5.2 Evaluation Criteria**

The application of the analysis framework proposed by Lynch (1998a, pp. 4-11) not only permitted the evaluation of the systems under investigation, but also provided an opportunity to assess the criteria themselves.

The conversion of the criteria from a narrative into evaluative elements for use in a survey and in interviews was challenging. Nonetheless the process provided insights about the methodology and the criteria themselves. The survey results,

for instance, suggested that some aspects of the framework may not have been fully understood by the respondents, such as cross-protocol flexibility. This not only reflected the respondents' knowledge but also the methods chosen to gather the evaluative data.

The exposition by Lynch of the analysis framework was extensive and thorough. The chosen criteria covered most, if not all, of the aspects that are crucial to any evaluative assessment, although some aspects were more prominent in the discussion than others. Despite their formation in 1998, the criteria are still valid, though the weighting or importance of some has changed following developments in access management technology.

One area of concern, particularly in relation to Shibboleth, is the cost (both financial and personnel) of implementation, as comments from an open-ended question in the survey indicated (see **Appendix H**). The issue of cost was recognised by Lynch (1998a, p. 21) during the formation of the analysis framework but, at that time, it was felt that there was insufficient data. Lynch added that there was 'an urgent need to develop a better basis for estimating the initial deployment and operating costs of the various approaches.' Should cost therefore be added to the analysis framework as an additional, and explicit, criterion? Unlike the other criteria, cost is not about functionality nor is it an overly objective issue, as costs inevitably vary from institution to institution. In that sense, whilst costs should necessarily be taken into account in any decision-making processes regarding access management systems, it should not be considered a formal element of the analysis framework, which should remain focused on functionality.

Sävilammi (1998) based his comparison of access management methods on the same analysis framework, albeit with different groupings (separating granularity from extensibility for instance). This may have been a reaction to the levels of detail within each of the seven aspects and an attempt to draw out areas of particular interest at that time. Indeed, one of the difficulties with the seven

groupings is the varying degrees of detail within each – a fact reflected in the structure of this study's survey. Rather than re-working the groupings, careful interpretation of the detail is more appropriate when utilising the analysis framework, a process that, in turn, allows easier comparison with previous studies. However, the issue of interpretation does remain a significant challenge in this methodology.

It is clear that some of the aspects being rated might have been assessed more effectively using other methodological tools. Interviews, used in this study to explore understandings and provide clarification, and group discussions might perhaps have been the more appropriate means of obtaining the majority of the evaluative data. The framework for analysis is exactly that – a framework. It did not provide a methodology, a means by which it could be applied to address all situations. Treated as a framework alone, the work by Lynch (1998a) does provide a sound basis upon which to commence an evaluative study. More work, however, needs to be carried out to determine the most appropriate methodological tools by which this framework can be utilised.

### **5.3 Policy Issues**

The developments in functionality since the early days of access management have given rise to a range of tools and statistical information for use by libraries. However, those same developments have also given rise to issues that are not technical in nature.

At the heart of these issues is the tension between privacy on the one hand and accountability and the collection of management data on other. This tension is at its most intense with Shibboleth, where strict privacy is at the heart of the system (see Internet2, 2006a). With little or no demographic information being conveyed to resource suppliers, the provision of usage statistics is adversely affected. The

lack of an integral statistics module within Shibboleth, due to its nature, also leaves institutions reliant on usage data from resource suppliers.

Shibboleth, as a federated identity model, does address this issue, however, with Attribute Release Policies (ARP). These provide control over the information released about users by their authenticating institution (known as the 'Identity Provider' (IdP) to resource suppliers (SP or 'Service Providers'). ARPs can be defined at various levels – institutional, communal (groups) or individual. Typically, Service Providers require certain user attributes (defined in a Service Description (SD) to be provided, as a result of the 'attribute request' step of the Shibboleth login process, in order to grant access to a certain service level and facilities. If individual users deny the release of certain attributes, they can do so with the result that a service may then not be available to them.

The implementation of access management systems, therefore, does require institutions to develop and regularly review policies on accountability and, in the case of Shibboleth, the release of attributes. These policies, particularly with the ARPs in Shibboleth, need to be placed within wider institutional strategies. In addition, the engagement with, and education of, users is crucial. Users already 'release' personal information when they register with some resources for personalisation services, even when using Athens. However, they need to be more aware of the value of the data held about them by their institutions and of the implications of the release of that information.

Education, too, is integral to security. As has been shown, the security of systems utilising existing institutional accounts is deemed greater, in part because the user has much more to lose if their account is compromised. However, the effectiveness of security is dependant on the users understanding their obligations and appreciating the risks to them, as well as their institution, in the event of compromise.



## **5.4 Summary**

The research has shown that the access management systems that utilised existing institutional accounts satisfied more of the requirements of a viable solution, as defined by Lynch (1998a), than those systems that required additional accounts.

The analysis framework was also demonstrated to be a viable basis for the assessment, although questions were raised about the suitability of some of the methodological tools used.

## 6. Conclusion

This chapter draws together the results of the survey and the interviews, together with the findings of the literature review, and addresses some of the issues raised, in keeping with the aims and objectives outlined in the **Introduction**.

### 6.1 Access Management Systems

The literature review underpinned the study in several significant ways. Importantly, it revealed the developing nature of access management systems, from IP address filtering to Eduserv Athens and Shibboleth, enabling the key systems for this study to be identified and evaluated.

The subsequent study of the four systems (the three forms of Athens plus Shibboleth) highlighted the significant differences in functionality between those systems that utilised existing institutional accounts (AthensDA and Shibboleth) and those that required additional credential sets (Athens Access and Personal Accounts). It was clear that those systems that interfaced with local SSO facilities met more of the requirements for a complete access management solution. Furthermore, the gradual separation of authentication from authorisation in access management could be seen in the transition from Eduserv Athens to solutions based on Shibboleth. In that sense, the developments are leading to a realisation of the priorities for a national access management system first outlined for JISC by Robiette (2000).

Recognition, however, that Shibboleth is not an access management *per se* but rather middleware, reliant on other systems for authentication and other functionality, perhaps made the comparison a little unbalanced, even if the mode of delivery to the user can share some characteristics of AthensDA. It is clear that Shibboleth in isolation is but one part of the story – and that will impact on any future assessment of its efficacy.

## **6.2 Evaluation Criteria**

The review also highlighted key issues within access management, particularly the tension between privacy and accountability, and identified several expositions of what was considered essential for an effective access management system. The review identified the framework for analysis proposed by Lynch in the 'White Paper' (1998a), the five aims of access management defined by Arms (1999, p. 25) and the priorities first defined for JISC (Robiette, 2000) as integral to the study. Furthermore, the 'White Paper', regarded by Robiette (2000) as 'the departure point for most...discussions of access management', was noted for its provision of common terminology but not for its adoption as an evaluative tool. The study sought to address this by deriving the assessment criteria for the research from the 'White Paper'.

This engagement with the analysis framework proved to be successful, enabling the objectives of the study to be met, whilst assessing the criteria themselves for continued applicability. However, the examination of a similar exercise by Sävilammi (1998), and experience from this research, suggested that the weighting or priority of particular issues within the framework at a given time could lead to incomparable studies, despite sharing the same starting point. The application of such a framework is also vulnerable to input, conscious or not, by the researcher through their subjective understanding of terms and the 'projecting' of their own concerns and priorities.

Overall, the 'White Paper' provided a useful set of criteria with which to assess access management systems, although some issues remain with its application.

## **6.3 Methodology**

With the analysis framework providing the criteria but not a methodology, a blended approach was adopted, with an emphasis on quantitative data acquisition via a survey, supported by qualitative input from interviews and research. Whilst

the use of a mixed methodology was appropriate, the nature of the criteria perhaps lent themselves more to qualitative research, or certainly a balanced division. The assessment of access management functionality is inevitably subjective and very dependant on understandings – something that can be more easily explored using qualitative tools.

The limited exposure of the survey sample to Shibboleth led to a low number of evaluations for that method. Furthermore, the unexpected delay in the wider release of ‘early adopter’ project final reports (still awaited at the time of writing) reduced the qualitative data available to the study. Whilst it was appropriate to include Shibboleth, its evaluation using the same analysis framework is an area for future research, perhaps once it has been more fully adopted within UK higher education. Input, too, from the NHS and further education might then also be appropriate.

#### **6.4 Summary**

Overall, this research was successful within the confines of the resources available to the researcher, and met all of the objectives. With the identification of a framework for analysis, and the observation of trends within access management, there is scope to build on this study as part of a future assessment of Shibboleth and any future access management systems.

## **7. Reflections**

This study has addressed its aims and objectives. However, there are some aspects of the topic and the process which, with hindsight, might have been done differently.

### **7.1 Sample**

It is clear that further education and the NHS (National Health Service) make extensive use of Eduserv Athens, and both sectors will be engaging with Shibboleth. It might therefore have been appropriate to widen the sample to include these constituencies.

### **7.2 Survey Design**

An additional screen could have been added to the start of the survey, to help ensure that respondents were only from higher education. It could have asked for the user to select their sector (further or higher education, NHS etc.) and then have directed only those from higher education to the questions.

### **7.3 Data Collection**

It might have been appropriate to carry out more interviews, to obtain additional qualitative data.

### **7.4 Shibboleth**

Whilst Shibboleth is integral to any discussion of access management, its limited implementation produced a small sample, thus restricting the ability to identify conclusive evidence. However, the exclusion of Shibboleth would have devalued this study.

## References and Bibliography

Akenti. (2004). *Akenti: Distributed Access Control*. [Online]. Available from: <http://www-itg.lbl.gov/Akenti/> [Accessed: 09 August 2006].

Allison, A. et al. (2005). Digital Identity Matters. *Journal of the American Society for Information Science and Technology*. 56 (4) pp.364-372.

ANGEL. (2005). *ANGEL: Authenticated Networked Guided Environment for Learning*. [Online]. Available from: <http://www.angel.ac.uk/ANGEL/> [Accessed: 09 August 2006].

Arms, C. (1999). *Enabling Access in Digital Libraries: a report on a workshop on access management*. [Online]. Washington, D.C., Council on Library and Information Resources. Available from: <http://www.clir.org/pubs/abstract/pub79.html> [Accessed: 10 August 2006].

Bordeiau, S. et al. (2000). Delivering Electronic Resources with Web OPACs and Other Web-Tools: Needs of reference librarians. *Reference Services Review*. [Online]. 28 (2), pp.111-118. Emerald. Available from: <http://www.emerald-library.com/ft> [Accessed: 02 November 2002].

Breeding, M. (2001). Offering Remote Access to Restricted Resources. *Information Today*. [Online]. 18 (5), pp.52-53. Available from: <http://www.findarticles.com/> [Accessed: 25 November 2002].

Bryman, A. (1988). *Quantity and Quality in Social Research*. London: Unwin Hyman.

Bryman, A (1993). Cited in: Burton, D. ed. (2000). *Research Training for Social Scientists*. London: Sage Publications. p. 299.

Burton, D. (2000a). Data Collection Issues in Survey Research. In: D. Burton. ed. *Research Training for Social Scientists*. London: Sage Publications.

Burton, D. (2000b). Design Issues in Survey Research. In: D. Burton. ed. *Research Training for Social Scientists*. London: Sage Publications.

Cain, M. (2003). Managing Technology: Cybertheft, network security, and the library without walls. *The Journal of Academic Librarianship*. [Online]. 29 (4) pp.245-248. EBSCO EJS. Available from: <http://ejournals.ebsco.com> [Accessed: 25 June 2006].

CANDLE-Athens Project. (2002). *Authentication and Authorization: a Guide – Glossary*. [Online]. Available from: <http://litc.sbu.ac.uk/candleathens/glossary.html> [Accessed: 10 November 2002].

CANDLE Project. (2002). *The CANDLE Project*. [Online]. Available from: <http://www.sbu.ac.uk/litc/candle/> [Accessed: 25 November 2002].

Cantor, S. & Erdos, M. (2002). *Shibboleth-Architecture DRAFT v05*. [Online]. Internet2. Available from: <http://shibboleth.internet2.edu/draft-internet2-shibboleth-arch-v05.html> [Accessed: 13 August 2006].

Carnevale, D. (2002). Security Lapses on Campuses Permit Theft from JSTOR Database. *The Chronicle of Higher Education*. [Online]. Issue 12. Available from: <http://chronicle.com/free/2002/12/2002121201t.htm> [Accessed: 12 August 2006].

Chambers, S. (2004). Access Management: the New Information Skill? *SCONUL Focus*. 32 (summer/autumn), pp.9-11.

Clark, E. (2003). Making Peace with Passwords. *IT Architect*. [Online]. October. Available from: <http://www.itarchitect.com/showArticle.jhtml?articleID=15201403> [Accessed: 16 July 2006].

Collins, M. & Ferguson, C. (2002). Context-Sensitive Linking: it's a small world after all. *Serials Review*. 28 (4), pp.267-282.

Cox, A. (2000). One Password for Everything. *Exploit Interactive*. [Online]. Issue 5. Available from: <http://www.exploit-lib.org/issue5/candle/> [Accessed: 09 August 2006].

Eales, S. (2002). How the Joint Information Systems Committee (JISC) is Working Towards Assisting Colleges to Better Support Part-Time and Distance Learners in Further Education. *ASSIGNation*. 19 (3), pp.9-12.

Eaton, J. (1998). Project HeadLine: Access control and authentication – issues for access to networked information resources. *The New Review of Academic Librarianship*. 4, pp.11-18.



Eduserv Athens. (2003). *Athens Wins JISC UK HE and FE Contract*. [Online]. 03 April. Available from: [http://www.athensams.net/news/jisc\\_contract2003.html](http://www.athensams.net/news/jisc_contract2003.html) [Accessed: 12 August 2006].

Eduserv Athens. (2006a). *Eduserv Athens*. [Online]. Available from: <http://www.athensams.net/> [Accessed: 09 August 2006].

Eduserv Athens. (2006b). *Athens Devolved Authentication*. [Online]. Available from: [http://www.athensams.net/local\\_auth/athensda/](http://www.athensams.net/local_auth/athensda/) [Accessed: 12 August 2006].

Eduserv Athens. (2006c). *Athens Organisations*. [Online]. Available from: <http://auth.athensams.net/orglist.php> [Accessed: 20 August 2006].

Fecko, M. (1997). *Electronic Resources: Access and issues*. London: Bowker-Saur.

Flick, U. (1998). *An Introduction to Qualitative Research*. London: Sage Publications.

Gambles, B., Thebridge, S. & Dalton, P. (2001). *The MIDLANDER Project: Final report*. Library and Information Commission Research Report 128. London: Resource - the Council for Museums, Archives and Libraries.

Garrison, W. & McClellan, G. (1997). Tao of Gateway: Providing internet access to licensed databases. *Library Hi Tech*. 15 (1-2), pp. 39-54.

Gephart, R. (1999). Paradigms and Research Methods. *Research Methods Forum*. [Online]. 4, pp.1-9. Available from: <http://division.aonline.org/rm/> [Accessed: 09 August 2006].

Gilmore, B. et al. (2004). *Core Middleware and Shared Services Studies: Single Sign-On Report*. [Online]. JISC. Available from: [http://www.jisc.ac.uk/uploaded\\_documents/CMSS-Gilmore.pdf](http://www.jisc.ac.uk/uploaded_documents/CMSS-Gilmore.pdf) [Accessed: 11 August 2006].

GLAM. (2003). *Global Access Management Project (GLAM)*. [Online]. Available from: <http://www.glam.lon.ac.uk/> [Accessed: 09 August 2006].

Goerwitz, R. (1998). Pass-Through Proxying as a Solution to the Off-Site Web-Access Problem. *D-Lib Magazine*. [Online]. Available from: <http://www.dlib.org/dlib/june98/stg/06goerwitz.html> [Accessed: 09 August 2006]

HeadLine website (2001). *Headline Home Page*. [Online]. Available from: <http://www.headline.ac.uk/> [Accessed: 09 August 2006].

Hepfer, C. & McElroy, E. (2004). A Man for All Reasons: An Interview with Clifford Lynch. *Serials Review*. [Online]. 30 (4) pp. 343-353. ScienceDirect. Available from: <http://www.sciencedirect.com/> [Accessed: 16 February 2006].

Hudomalj, E. & Jauk, A. (2006). Authentication and Authorisation Infrastructure for the Mobility of Users of Academic Libraries. *Program*. [Online]. 40 (1) pp.63-73. Emerald. Available from: <http://www.emeraldinsight.com/0033-0337.htm> [Accessed: 01 July 2006].

Internet2. (2006a). *Shibboleth Project – Internet2 Middleware*. [Online]. Available from: <http://shibboleth.internet2.edu/> [Accessed: 12 August 2006].

Internet2. (2006b). *Shibboleth Technical Introduction*. [Online]. Available from: <http://shibboleth.internet2.edu/tech-intro.html> [Accessed: 13 August 2006].

JISC. (1996). *Technologies to Support Authentication in Higher Education v5*. [Online]. Available from: [http://www.jisc.ac.uk/index.cfm?name=acn\\_support\\_authent](http://www.jisc.ac.uk/index.cfm?name=acn_support_authent) [Accessed: 09 August 2006].

JISC. (2002a). *Funding 04/02 - Access Management Service for UK Higher and Further Education*. [Online]. Available from: [http://www.jisc.ac.uk/index.cfm?name=funding\\_4\\_02](http://www.jisc.ac.uk/index.cfm?name=funding_4_02) [Accessed: 09 August 2006].

JISC. (2002b). *Circular 06/02 – Call for Projects in Authentication and Authorisation*. [Online]. Available from: [http://www.jisc.ac.uk/index.cfm?name=circular\\_06\\_02](http://www.jisc.ac.uk/index.cfm?name=circular_06_02) [Accessed: 09 August 2006].

JISC. (2004a). *Authentication, Authorisation and Accounting (AAA) Programme*. [Online]. Available from: [http://www.jisc.ac.uk/index.cfm?name=programme\\_aaa](http://www.jisc.ac.uk/index.cfm?name=programme_aaa) [Accessed: 09 August 2006].

JISC. (2004b). *Circular 1/04: Call for Projects in Core Middleware*. [Online]. Available from: [http://www.jisc.ac.uk/index.cfm?name=c01\\_04](http://www.jisc.ac.uk/index.cfm?name=c01_04) [Accessed: 03 June 2006].

JISC. (2004c). *The Future Position on Athens and Shibboleth*. [Online]. Available from:

[http://www.jisc.ac.uk/index.cfm?name=jisc\\_athens\\_shibboleth\\_pos\\_news050804](http://www.jisc.ac.uk/index.cfm?name=jisc_athens_shibboleth_pos_news050804)  
[Accessed: 03 June 2006].

JISC. (2004d). *Middleware Technology Programme to Draw Expertise from Further and Higher Education*. [Online]. Available from:

[http://www.jisc.ac.uk/index.cfm?name=middleware\\_proj\\_annouce\\_news\\_130504](http://www.jisc.ac.uk/index.cfm?name=middleware_proj_annouce_news_130504)  
[Accessed: 13 August 2006].

JISC. (2004e). *Core Middleware: Technology Development Projects Funded*. [Online]. Available from:

[http://www.jisc.ac.uk/index.cfm?name=middleware\\_announce](http://www.jisc.ac.uk/index.cfm?name=middleware_announce) [Accessed: 13 August 2006].

JISC. (2004f). *Core Middleware Inputs: Current Situation*. [Online]. Available from:

[http://www.jisc.ac.uk/index.cfm?name=middlewarerepp\\_inputs](http://www.jisc.ac.uk/index.cfm?name=middlewarerepp_inputs) [Accessed: 13 August 2006].

JISC. (2004g). *Circular 11/04: Core Middleware – Early Adopters Call for Proposals*. [Online]. Available from:

[http://www.jisc.ac.uk/index.cfm?name=funding\\_circular11\\_04](http://www.jisc.ac.uk/index.cfm?name=funding_circular11_04) [Accessed: 11 August 2006].

JISC. (2005). *Connecting People to Resources: Athens and Shibboleth*. [Online]. Available from:

[http://www.jisc.ac.uk/uploaded\\_documents/CMRoadmap03\\_05.doc](http://www.jisc.ac.uk/uploaded_documents/CMRoadmap03_05.doc) [Accessed: 10 August 2006].

JISC. (2006a). *JISC Announces the Development of a New Access Management System for the UK*. [Online]. Available from: [http://www.jisc.ac.uk/printer\\_friendly.cfm?name=news\\_shibboleth](http://www.jisc.ac.uk/printer_friendly.cfm?name=news_shibboleth) [Accessed: 13 August 2006].

JISC. (2006b). *JISC is Pleased to Announce the Development of a New Access Management Infrastructure for the UK Educational Sector*. [Online]. Available from: <http://www.jisc.ac.uk/index.cfm?name=federation> [Accessed: 03 June 2006].

JISC. (2006c). *Shibboleth: Connecting people to resources*. [Online]. Available from: [http://www.jisc.ac.uk/uploaded\\_documents/JISC-BP-Shibboleth.pdf](http://www.jisc.ac.uk/uploaded_documents/JISC-BP-Shibboleth.pdf) [Accessed: 13 August 2006].

JISC. (2006d). *Connecting People to Resources – Federated access management: JISC guide for institutions*. [Online]. Available from: [http://www.jisc.ac.uk/uploaded\\_documents/JISC-BP-ShibFedAcc-Inst.pdf](http://www.jisc.ac.uk/uploaded_documents/JISC-BP-ShibFedAcc-Inst.pdf) [Accessed: 13 August 2006].

JISC. (2006e). *Connecting People to Resources – Federated access management: JISC guide for publishers and service providers*. [Online]. Available from: [http://www.jisc.ac.uk/uploaded\\_documents/JISC-BP-ShibFedAcc-PubSP.pdf](http://www.jisc.ac.uk/uploaded_documents/JISC-BP-ShibFedAcc-PubSP.pdf) [Accessed: 13 August 2006].

JISC. (2006f). *Connecting People to Resources*. *JISC Inform.* 9, pp.11-14.

JISC. (2006g). *Interview: Online Publishers Embrace Federated Access Management*. [Online]. Available from: [http://www.jisc.ac.uk/index.cfm?name=accman\\_publishers](http://www.jisc.ac.uk/index.cfm?name=accman_publishers) [Accessed: 10 August 2006].

JISC. (2006h). JISC Letter to Institutions. [Online]. Available at: [http://www.jisc.ac.uk/uploaded\\_documents/Shibb-institution-letter.pdf](http://www.jisc.ac.uk/uploaded_documents/Shibb-institution-letter.pdf) [Accessed: 13 August 2006].

JISC Monitoring Unit. (2006a). *JISC Monitoring Unit Website*. [Online]. Available from: <http://www.mu.jisc.ac.uk/> [Accessed: 08 August 2006].

JISC Monitoring Unit. (2006b). *Annual Survey of Network Content Services 2005/2006*. [Online]. Available at: <http://www.mu.jisc.ac.uk/surveys/ncs2005/> [Accessed: 26 August 2006].

Klingenstein, N. (2004). Primers on Standards: Shibboleth. *Computers in Libraries*. [Online]. 24 (2), pp. 18-31. Available from: <http://www.infoday.com/cilmag/feb04/primers.shtml> [Accessed: 10 August 2006].

Lam, V-T. (2000). Organizational and Technical Issues in Providing Access to Electronic Journals. *The Serials Librarian*. 39 (3) pp.25-34.

Liberty Alliance. (2006). *Liberty Alliance Project – Digital Identity Defined*. [Online]. Available from: <http://www.projectliberty.org/> [Accessed: 13 August 2006].

Lynch, C. (1997). The Changing Role in a Networked Information Environment. *Library Hi Tech*. 15 (1-2), pp. 30-38.

Lynch, C. (1998a). *A White Paper on Authentication and Access Management Issues in Cross-Organizational Use of Networked Information Resources*. [Online]. Washington D.C., Coalition for Networked Information. Available from: <http://www.cni.org/projects/authentication/authentication-wp.html> [Accessed: 09 August 2006].

Lynch, C. (1998b). Access Management for Networked Information Resources. *ARL Newsletter*. [Online]. 201. Available from: <http://www.arl.org/newsltr/201/> [Accessed: 09 August 2006].

Lynch, C. (1999). Authentication and Trust in a Networked World. *Educom Review*. [Online]. 34 (4). Available from: <http://www.educause.edu/ir/library/html/erm/erm99/erm994a.html> [Accessed: 09 August 2006].

Lynch, C. (2000). Authenticity and Integrity in the Digital Environment: an exploratory analysis of the central role of trust. In: *Authenticity in a Digital Environment*. Washington D.C.: Council on Library and Information Resources.

MAMS. (2006). *MAMS: Meta Access Management System – Testbed Federation*. [Online]. Available from: <http://www.federation.org.au/FedManager/jsp/index.jsp> [Accessed: 12 August 2006].

Martin, M. et al. (2002). Federated Digital Rights Management. *D-Lib Magazine*. [Online]. July/August. Available from:  
<http://www.dlib.org/dlib/july02/martin/07martin.html> [Accessed: 09 August 2006].

Maykut, P. & Morehouse, R. (1994). *Beginning Qualitative Research: a philosophical and practical guide*. London: Falmer Press.

McLean, N. (2000). Matching People and Information Resources: Authentication, authorisation and access management and experiences at Macquarrie University, Sydney. *Program*. 34 (3), pp.239-255.

Microsoft. (2006). *Windows CardSpace (formerly 'InfoCard')*. [Online]. Available from: <http://msdn.microsoft.com/winfx/reference/infocard/default.aspx> [Accessed 13 August 2006].

Millman, D. (1999). Cross-Organizational Access Management. *D-Lib Magazine*. [Online]. November. Available from:  
<http://www.dlib.org/dlib/november99/millman/11millman.html> [Accessed: 09 August 2006].

Moyo, L. (2002). Collections on the Web: Some access and navigation issues. *Library Collections, Acquisitions & Technical Services*. 26, pp.47-59.

Needleman, M. (2004). The Shibboleth Authentication/Authorization System. *Serials Review*. [Online]. 30 (3) pp.252-253. ScienceDirect. Available from:  
<http://www.sciencedirect.com/> [Accessed: 16 February 2006].



NISO. (2005). *Task Group 1 Access Management*. [Online]. Available from: [http://www.lib.ncsu.edu/niso-mi/index.php/Task\\_Group\\_1\\_Access\\_Management](http://www.lib.ncsu.edu/niso-mi/index.php/Task_Group_1_Access_Management) [Accessed: 12 August 2006].

Norris, L. (2004). Facilitating Access to E-Resources with Eduserv Athens. *Serials*. [Online]. 17 (3) pp.277-279. EBSCO EJS. Available from: <http://ejournals.ebsco.com> [Accessed: 19 June 2006].

PAPI. (2005). *The PAPI AA Framework*. [Online]. Available from: <http://papi.rediris.es/> [Accessed: 09 August 2006].

Paschoud, J. (1999a). All Users Are Not Created Equal! How to decide who gets what from your hybrid library. *Internet Librarian International Conference Proceedings*. [Online]. Available from: <http://hdl.handle.net/1988/17> [Accessed: 01 July 2006].

Paschoud, J. (1999b). The Problems of Securing Internet Access to Electronic Documents...and a Solution! *Vine*. 112, pp.16-21.

Paschoud, J. (2004). Shibboleth and SAML: at last a viable global standard for resource access management. *New Review of Information Networking*. [Online]. 10 (2) pp. 147-159. Swetswise. Available from: <http://www.swetswise.com/> [Accessed: 01 July 2006].

Patton, M. (2002). *Qualitative Research and Evaluation Methods*. 3<sup>rd</sup> edition. London: Sage.

Pinfield, S. et al. (1998). Realizing the Hybrid Library. *D-Lib Magazin*. October. [Online]. Available from: <http://www.dlib.org/dlib/october98/10pinfield.html> [Accessed: 09 August 2006].

Pinto, F. & Fraser, M. (2003). Access Management, the Key to a Portal. *Ariadne*. [Online]. 35. Available from: <http://www.ariadne.ac.uk/issue35/SPP/intro.html> [Accessed: 10 August 2006].

Potter, L. (1999). *User Passports and Visas: Understanding the role of identification metadata*. Library and Information Commission Research Report 22. London: Book Industry Communication.

Ritchie, J. & Lewis, J. eds. (2003). *Qualitative Research Practice*. London: Sage Publications.

Robiette, A. (2000). *Sparta: the second-generation access management system for UK further and higher education*. [Online]. JISC. Available from: [http://www.jisc.ac.uk/index.cfm?name=jcie\\_sparta](http://www.jisc.ac.uk/index.cfm?name=jcie_sparta) [Accessed: 09 August 2006].

Robiette, A. (2001a). Digital Certificates and Public Key Infrastructure. *Vine*. 123, pp.42-49.

Robiette, A. (2001b). Managing Access to Electronic Information: Progress and prospects. *Serials*. 14 (3), pp.301-304.

Robiette, A. (2002a). *The Future of Authentication for JISC Services: a consultation paper*. [Online]. JISC. Available from: [http://www.jisc.ac.uk/index.cfm?name=jcie\\_authentication](http://www.jisc.ac.uk/index.cfm?name=jcie_authentication) [Accessed: 09 August 2006].

Robiette, A. (2002b). *Middleware for the JISC Information Environment: Proposals for discussion*. [Online]. JISC. Available from: [http://www.jisc.ac.uk/index.cfm?name=jcie\\_middleware](http://www.jisc.ac.uk/index.cfm?name=jcie_middleware) [Accessed: 09 August 2006].

Robiette, A. (2002c). *X.509 Certificates: Frequently asked questions*. [Online]. JISC. Available from: [http://www.jisc.ac.uk/index.cfm?name=jcie\\_x509](http://www.jisc.ac.uk/index.cfm?name=jcie_x509) [Accessed: 09 August 2006].

Rusbridge, C. (1998). Towards the Hybrid Library. *D-Lib Magazine*. [Online]. July/August. Available from: <http://www.dlib.org/dlib/july98/rusbridge/07rusbridge.html> [Accessed: 09 August 2006].

Sävilammi, J. (1998). *Access Management Problem: Definitions and considerations*. [Online]. Available from: <http://www.tml.tkk.fi/Opinnot/Tik-110.501/1998/papers/8accessmanag/accessmanag.html> [Accessed: 12 August 2006].

SECURE Project. (2005). *Secure Environment for Certificated Use of Resources*. [Online]. Available from: <http://www.angel.ac.uk/SECURE/> [Accessed: 09 August 2006].

SERENATE. (2003). *Summary Report on SERENATE Studies (D21)* [Online]. Available from: <http://www.serenate.org/publications/d21-serenate.pdf> [Accessed: 16 July 2006].

Smith, N. (2000). Inside the Digital Library. *Exploit Interactive*. [Online]. Issue 5. Available from: <http://www.exploit-lib.org/issue5/fd/> [Accessed: 09 August 2006].

Stroh, M. (2000). Qualitative Interviewing. In: D. Burton. ed. *Research Training for Social Scientists*. London: Sage Publications.

SWISh. (2006). *SWISh: South West Implementation of Shibboleth*. [Online]. Available from: <http://www.projects.ex.ac.uk/swish> [Accessed: 10 August 2006].

SWITCH. (2006). *SWITCH – NetServices – Authentication and Authorization Infrastructure (AAI)*. [Online]. Available from: <http://www.switch.ch/aai/> [Accessed: 12 August 2006].

TERENA. (2000). *TF-AACE (authentication and authorisation coordination for Europe) – terms of reference*. [Online]. Available from: <http://www.terena.nl/activities/tf-aace/tf-aace-tor.html> [Accessed: 09 August 2006].

TERENA. (2004). *TERENA Task Force on Authentication and Authorisation Coordination in Europe (TF-AACE) – Final Report*. [Online]. Available from: <http://www.terena.nl/activities/tf-aace/Del/TFAACE-FinalReportv-2.pdf> [Accessed: 10 August 2006].

Tilsed, I. & Johnson, N. (2006) *SWISh: Final Project Report*. [Online]. SWISh. Available from: <http://www.projects.ex.ac.uk/swish/SWIShFinalReport.pdf> [Accessed: 14 August 2006].

Wiseman, N. (1998). Implementing a National Access Management System for Electronic Services. *D-Lib Magazine*. [Online]. March. Available from: <http://dlib.ukoln.ac.uk/dlib/march98/wiseman/03wiseman.html> [Accessed: 10 August 2006].

Yeates, R. & Cox, A. (1999). Managing Networked Information Resources More Effectively: Candle. *Vine*. 112, pp.22-29.

# Appendices

**Appendix A** Survey Design

**Appendix B** Example E-Mail

**Appendix C** Interview Schedule

**Appendix D** Roles and Allegiances: Open Responses

**Appendix E** Survey Results Tables

**Appendix F** Priorities in an Access Management System: Table

**Appendix G** Comparative Analysis: Table

**Appendix H** Respondent Comments

# Appendix A

## Survey Design

---

## 1. Introduction

Hello,

Firstly, welcome to my survey!

This survey is part of some research I am undertaking for the dissertation of an MSc in Information & Library Management at the University of Central England in Birmingham.

For my research I am studying the current and proposed access management systems for electronic resources in UK Higher Education. In essence, this means the study of Eduserv Athens (in both the 'classic' and 'devolved' forms) and alternatives based on Shibboleth.

As an Athens Administrator myself I do appreciate how busy you are so I will be very grateful for any information you can provide to assist me in this endeavour.

For encouragement there is a draw (optional), in which respondents are invited to take part , for a £20 Amazon.co.uk gift certificate - details are on the closing screen. The winner will be decided by random selection within 24 hours of the survey close.

Any survey submissions will be used anonymously in my research, without any disclosure of the individual or institution.

Please note - the survey will guide you through the screens based on your answers. If you select 'No' to some answers you will jump those sections which are not applicable to you.

This survey will close at 9 pm on Friday 25th August.

Many thanks.

Ian Tilsed



# Access Management Systems for Electronic Resources in UK HE

[Exit this survey >>](#)

## 2. Section A: Who are you?

**\* 1. What is your role in relation to access management for electronic resources at your institution?**

- Athens Administrator (or member of the Athens Administration Team for your institution)
- Technical Developer
- Other (please specify)

**\* 2. Which department do you work for?**

- Library Services
- IT Services
- A Converged Service
- Other (please specify) \_\_\_\_\_

[<< Prev](#)      [Next >>](#)

**3. Section B: Eduserv Athens**

\* 3. Does your institution currently use, or has it ever used, Eduserv Athens as a means of controlling access to electronic resources?

Yes

No

<< Prev      Next >>

## **Access Management Systems for Electronic Resources in UK HE**

**Exit this survey >>**

### **4. Section B: Eduserv Athens - Access Accounts**

**\* 4. Does your institution currently use, or has it ever used, Athens Access Accounts\*?**

**(\* these are typically site-wide or departmental accounts, where access to resources is based on both the correct username/password and on the client's IP address; they can also be used by clients to create personal accounts)**

Yes

No

**<< Prev      Next >>**

# Access Management Systems for Electronic Resources in UK HE

[Exit this survey >>](#)

## 5. Section B: Eduserv Athens - Access Accounts

\* 5. Please rate the following aspects of Athens Access Accounts:

(a numeric scale is used, where 5 = Excellent, 4 = Good, 3 = Satisfactory, 2 = Mediocre, 1 = Poor)

	5	4	3	2	1
ease of implementation	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
suitability for distance users	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ability to include other sites within the institution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ease of maintenance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
control of access to resources by class or group level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
flexibility to cope with more users and/or a changed organisational structure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
effective for a wide range of network protocols	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
protect the privacy of the user	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
permit individual user accountability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
collection of management (usage) data - at user level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
collection of management (usage) data - at resource level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suitability for users with affiliations to multiple institutions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

[<< Prev](#)

[Next >>](#)

**6. Section B: Eduserv Athens - Personal Accounts**

\* 6. Does your institution currently use, or has it ever used, Personal Athens Accounts?

Yes

No

[<< Prev](#)      [Next >>](#)

# Access Management Systems for Electronic Resources in UK HE

[Exit this survey >>](#)

## 7. Section B: Eduserv Athens - Personal Accounts

\* 7. Please rate the following aspects of Athens Personal Accounts:

(a numeric scale is used, where 5 = Excellent, 4 = Good, 3 = Satisfactory, 2 = Mediocre, 1 = Poor)

	5	4	3	2	1
ease of implementation	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suitability for distance users	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ability to include other sites within the institution	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ease of maintenance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
control of access to resources by class or group level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
flexibility to cope with more users and/or a changed organisational structure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
effective for a wide range of network protocols	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
protect the privacy of the user	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
permit individual user accountability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
collection of management (usage) data - at user level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
collection of management (usage) data - at resource level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suitability for users with affiliations to multiple institutions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

[<< Prev](#)

[Next >>](#)

**8. Section B: Eduserv Athens - AthensDA**

\* 8. Does your institution currently use, or has it ever used, AthensDA?

Yes

No

[<< Prev](#)      [Next >>](#)

# Access Management Systems for Electronic Resources in UK HE

[Exit this survey >>](#)

## 9. Section B: Eduserv Athens - AthensDA

\* 9. Please rate the following aspects of AthensDA:

(a numeric scale is used, where 5 = Excellent, 4 = Good, 3 = Satisfactory, 2 = Mediocre, 1 = Poor)

	5	4	3	2	1
ease of implementation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suitability for distance users	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ability to include other sites within the institution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ease of maintenance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
control of access to resources by class or group level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
flexibility to cope with more users and/or a changed organisational structure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
effective for a wide range of network protocols	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
protect the privacy of the user	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
permit individual user accountability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
collection of management (usage) data - at user level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
collection of management (usage) data - at resource level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suitability for users with affiliations to multiple institutions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

[<< Prev](#)

[Next >>](#)



**10. Section C: Solution based on Shibboleth**

**\* 10. Does your institution currently use, or has it ever used, an access management solution based on Shibboleth as a means of controlling access to electronic resources?**

Yes

No

**<< Prev      Next >>**

# Access Management Systems for Electronic Resources in UK HE

[Exit this survey >>](#)

## 11. Section C: Solution based on Shibboleth

\* 11. Please rate the following aspects of a solution based on Shibboleth:

(a numeric scale is used, where 5 = Excellent, 4 = Good, 3 = Satisfactory, 2 = Mediocre, 1 = Poor)

	5	4	3	2	1
ease of implementation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suitability for distance users	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ability to include other sites within the institution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ease of maintenance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
control of access to resources by class or group level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
flexibility to cope with more users and/or a changed organisational structure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
effective for a wide range of network protocols	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
protect the privacy of the user	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
permit individual user accountability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
collection of management (usage) data - at user level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
collection of management (usage) data - at resource level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suitability for users with affiliations to multiple institutions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

[<< Prev](#)

[Next >>](#)

# Access Management Systems for Electronic Resources in UK HE

[Exit this survey >>](#)

## 12. Section D: Priorities & Overall Assessment

**\* 12. Please RANK the following factors in order of importance to you, 1 being the most important and 11 being the least. All attributes must be ranked.**

	1	2	3	4	5	6	7	8	9	10	11
Ease of Implementation	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Facilities for Distance Learners	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ease of Maintenance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>		<input checked="" type="radio"/>	<input type="radio"/>
Strong Security	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fine Granularity (e.g. assigning resources to classes)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Flexibility to Cope with Changes & Additions	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cross Platform Functionality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
User Privacy	<input checked="" type="radio"/>	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Individual User Accountability	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Collection of Management Data	<input type="radio"/>	<input type="radio"/>			<input type="radio"/>	<input type="radio"/>		<input type="radio"/>		<input checked="" type="radio"/>	<input checked="" type="radio"/>
Facilities for	<input checked="" type="radio"/>	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>		<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Users with  
Affiliations to  
Multiple  
Institutions

**\* 13. How do you rate the following in terms of providing what you need to control access to your institution's electronic resources?**

**(a numeric scale is used, where 5 = Excellent, 4 = Good, 3 = Satisfactory, 2 = Mediocre, 1 = Poor)**

	5	4	3	2	1	N/A
Eduserv Athens - Access Accounts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Eduserv Athens - Personal Accounts	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Eduserv Athens - AthensDA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Shibboleth Solution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**<< Prev      Next >>**

**13. Section E: Survey Conclusion**

This is the final page of the survey.

If you have any comments you would like to make on this survey, or the issues raised by it, please use the space at the bottom of this screen.

Thank you for sparing the time to complete this survey - your effort is very much appreciated.

**14. To enter the draw for a £20 Amazon.co.uk gift certificate, please enter your name and e-mail address below:**

**15. In the event that you should be the lucky winner of the draw, would you be happy to be identified as such in any subsequent announcement about the survey?**

Yes

No



**Optional feedback and comments:**

# Appendix B

## Example E-Mail

---

## Appendix B – Example E-Mail

(please excuse cross-posting)

This message is directed to Electronic Resource Librarians, Athens Administrators & Technical Implementers/Developers of Access Management Solutions in UK HIGHER EDUCATION - please forward as appropriate.

-----

Hello,

I am conducting a survey as part of some research I am undertaking for the dissertation of an MSc in Information & Library Management at the University of Central England in Birmingham.

For my research I am evaluating the current and proposed access management systems for electronic resources in UK Higher Education. In essence, this means the study of Eduserv Athens (in both the 'classic' and 'devolved' forms) and alternatives based on Shibboleth.

As an Athens Administrator (and a Shibboleth project manager) myself I do appreciate how busy you are so I will be very grateful for any information you can provide to assist me in this endeavour. To take part in the survey (which takes about 10 minutes to complete) please select the following link:

<http://www.surveymonkey.com/s.asp?u=852182451089>

For encouragement there is a draw (optional), in which respondents are invited to take part, for a £20 Amazon.co.uk gift certificate.

Any survey submissions will be used anonymously in my research, without any disclosure of the individual or institution.

This survey will close at 9 pm on Friday 25th August.

Many thanks, in advance, for your help.

Ian Tilsed  
University of Exeter

# Appendix C

## Interview Schedule

---



## **Appendix C – Interview Schedule**

Explain the purpose of the survey and why they have been chosen.

### **Opening Question:**

What do you understand the term 'access management' to mean?

### **Main Questions:**

What are your opinions on the ease or otherwise of implementation and maintenance of the [Eduserv Athens / Shibboleth] system?

In the context of access management what do you understand 'secure' to mean?

Applying that definition, how secure do you think the [Eduserv Athens / Shibboleth] system is, for both the institution and the user?

Does [Eduserv Athens / Shibboleth] offer any level of fine grained access control (explain) and, if so, how effective do you rate this functionality?

To what extent, if any, can [Eduserv Athens / Shibboleth] be said to protect a user's privacy?

The other side of the privacy discussion is the notion of accountability (tracing someone when they have contravened a licence condition, for instance) – to what extent, if any, does [Eduserv Athens / Shibboleth] permit this by the institution?

To an institution, the collection of management data is crucial in the decision-making process – how well does [Eduserv Athens / Shibboleth] address this need?

**Closing Summary:**

What do you see as the most important aspects of an access management system for UK higher education?

# Appendix D

## Roles and Allegiances: Open Responses

---

## Appendix D – Roles and Allegiances: Open Responses

### Roles

---

Shibboleth implementation team

Manager

Athens Administration team AND technical developer

eresources librarian

Integration architect

Administration and alerting

Senior LIS Officer (Electronic Resources)

Manager

subject librarian

library staff - testing of new methods

Athens Admin & Developer

ATHENS administrator for NHS staff but not for University

Both

Manager

Advisor - researcher

Athens DSP/LA support

Systems Librarian

IT / project manager

Line manager of our Athens Administrator

Technical Services Manager

Library Projects Manager

marketing

### **Departmental Allegiances**

---

ILT Development

Archive

e-Services Integration

Learning and Information Services

Academic Support Tutor (HE)

Grid

Athens support

Arts & Humanities Data Service (hosted by King's College London)

marketing

Advisory Group

# Appendix E

## Survey Results Tables

---

## Appendix E – Survey Results Tables

Tables compiled from survey statistical output, indicating comparative ranking.

**Table E1 Rating: Ease of Implementation**

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens:</b> <b>Access Accounts</b>	19% (12)	47% (29)	24% (15)	8% (5)	2% (1)
<b>Athens:</b> <b>Personal Accounts</b>	21% (15)	47% (34)	27% (20)	5% (4)	0% (0)
<b>Athens:</b> <b>AthensDA</b>	12% (4)	41% (13)	34% (11)	9% (3)	3% (1)
<b>Shibboleth</b>	11% (1)	33% (3)	33% (3)	0% (0)	22% (2)

**Table E2 Rating: Suitability for Distance Users**

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens:</b> <b>Access Accounts</b>	21% (13)	19% (12)	16% (10)	13% (8)	31% (19)
<b>Athens:</b> <b>Personal Accounts</b>	41% (30)	38% (28)	15% (11)	4% (3)	1% (1)
<b>Athens:</b> <b>AthensDA</b>	41% (13)	47% (15)	6% (2)	6% (2)	0% (0)
<b>Shibboleth</b>	33% (3)	44% (4)	22% (2)	0% (0)	0% (0)

---

**Table E3 Rating: Ease of Maintenance**

---

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens:</b> <b>Access Accounts</b>	19% (12)	29% (18)	37% (23)	13% (8)	2% (1)
<b>Athens:</b> <b>Personal Accounts</b>	15% (11)	41% (30)	23% (17)	18% (13)	3% (2)
<b>Athens:</b> <b>AthensDA</b>	38% (12)	28% (9)	31% (10)	3% (1)	0% (0)
<b>Shibboleth</b>	22% (2)	22% (2)	33% (3)	11% (1)	11% (1)

---

**Table E4 Rating: Security**

---

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens:</b> <b>Access Accounts</b>	15% (9)	34% (21)	27% (17)	18% (11)	6% (4)
<b>Athens:</b> <b>Personal Accounts</b>	18% (13)	44% (32)	25% (18)	12% (9)	1% (1)
<b>Athens:</b> <b>AthensDA</b>	41% (13)	53% (17)	6% (2)	0% (0)	0% (0)
<b>Shibboleth</b>	44% (4)	56% (5)	0% (0)	0% (0)	0% (0)



---

**Table E5 Rating: Ability to Include Other Sites within the Institution**

---

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens:</b> <b>Access Accounts</b>	8% (5)	27% (17)	40% (25)	16% (10)	8% (5)
<b>Athens:</b> <b>Personal Accounts</b>	22% (16)	41% (30)	26% (19)	8% (6)	3% (2)
<b>Athens:</b> <b>AthensDA</b>	31% (10)	38% (12)	28% (9)	3% (1)	0% (0)
<b>Shibboleth</b>	33% (3)	22% (2)	44% (4)	0% (0)	0% (0)

---

**Table E6 Rating: Control of Access to Resources by Class / Group Level**

---

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens:</b> <b>Access Accounts</b>	11% (7)	42% (26)	35% (22)	6% (4)	5% (3)
<b>Athens:</b> <b>Personal Accounts</b>	10% (7)	48% (35)	26% (19)	14% (10)	3% (2)
<b>Athens:</b> <b>AthensDA</b>	19% (6)	47% (15)	25% (8)	9% (3)	0% (0)
<b>Shibboleth</b>	22% (2)	67% (6)	11% (1)	0% (0)	0% (0)

**Table E7 Rating: Flexibility to Cope with More Users / Changed Structure**

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens:</b> <b>Access Accounts</b>	8% (5)	31% (19)	42% (26)	13% (8)	6% (4)
<b>Athens:</b> <b>Personal Accounts</b>	12% (9)	41% (30)	38% (28)	7% (5)	1% (1)
<b>Athens:</b> <b>AthensDA</b>	25% (8)	50% (16)	22% (7)	3% (1)	0% (0)
<b>Shibboleth</b>	22% (2)	56% (5)	11% (1)	11% (1)	0% (0)

**Table E8 Rating: Suitability for Users with Multiple Institution Affiliations**

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens:</b> <b>Access Accounts</b>	5% (3)	13% (8)	43% (26)	23% (14)	16% (10)
<b>Athens:</b> <b>Personal Accounts</b>	12% (9)	32% (23)	32% (23)	12% (9)	12% (9)
<b>Athens:</b> <b>AthensDA</b>	19% (6)	16% (5)	31% (10)	28% (9)	6% (2)
<b>Shibboleth</b>	33% (3)	22% (2)	44% (4)	0% (0)	0% (0)

**Table E9 Rating: Effective for a Wide Range of Network Protocols**

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens: Access Accounts</b>	8% (5)	24% (15)	53% (33)	13% (8)	2% (1)
<b>Athens: Personal Accounts</b>	11% (8)	38% (28)	42% (31)	5% (4)	3% (2)
<b>Athens: AthensDA</b>	28% (9)	31% (10)	34% (11)	3% (1)	3% (1)
<b>Shibboleth</b>	22% (2)	33% (3)	33% (3)	0% (0)	11% (1)

**Table E10 Rating: Protect the Privacy of the User**

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens: Access Accounts</b>	10% (6)	47% (29)	34% (21)	6% (4)	3% (2)
<b>Athens: Personal Accounts</b>	12% (9)	49% (36)	30% (22)	4% (3)	4% (3)
<b>Athens: AthensDA</b>	41% (13)	41% (13)	19% (6)	0% (0)	0% (0)
<b>Shibboleth</b>	56% (5)	44% (4)	0% (0)	0% (0)	0% (0)

**Table E11 Rating: Permit Individual User Accountability**

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens: Access Accounts</b>	6% (4)	34% (21)	26% (16)	10% (6)	24% (15)
<b>Athens: Personal Accounts</b>	27% (20)	42% (31)	30% (22)	0% (0)	0% (0)
<b>Athens: AthensDA</b>	38% (12)	38% (12)	19% (6)	6% (2)	0% (0)
<b>Shibboleth</b>	22% (2)	67% (6)	11% (1)	0% (0)	0% (0)

**Table E12 Rating: Collection of Management Data – User Level**

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens: Access Accounts</b>	10% (6)	16% (10)	37% (23)	19% (12)	18% (11)
<b>Athens: Personal Accounts</b>	15% (11)	53% (39)	25% (18)	5% (4)	1% (1)
<b>Athens: AthensDA</b>	19% (6)	25% (8)	50% (16)	3% (1)	3% (1)
<b>Shibboleth</b>	11% (1)	44% (4)	22% (2)	22% (2)	0% (0)

**Table E13: Collection of Management Data – Resource Level**

	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
<b>Athens: Access Accounts</b>	13% (8)	23% (14)	<b>50%</b> <b>(31)</b>	8% (5)	6% (4)
<b>Athens: Personal Accounts</b>	15% (11)	<b>55%</b> <b>(40)</b>	29% (21)	1% (1)	0% (0)
<b>Athens: AthensDA</b>	19% (6)	28% (9)	<b>47%</b> <b>(15)</b>	6% (2)	0% (0)
<b>Shibboleth</b>	11% (1)	33% (3)	11% (1)	<b>44%</b> <b>(4)</b>	0% (0)

# Appendix F

## Priorities in Access Management Systems: Table

---

## Appendix F – Priorities in Access Management: Table

	1	2	3	4	5	6	7	8	9	10	11	Response Average
Ease of Implementation	<b>28% (19)</b>	23% (16)	12% (8)	12% (8)	1% (1)	4% (3)	4% (3)	4% (3)	3% (2)	7% (5)	1% (1)	<b>3.68</b>
Facilities for Distance Learners	<b>19% (13)</b>	16% (11)	15% (10)	9% (6)	7% (5)	4% (3)	9% (6)	9% (6)	4% (3)	3% (2)	4% (3)	<b>4.44</b>
Ease of Maintenance	17% (12)	<b>28% (19)</b>	20% (14)	12% (8)	7% (5)	6% (4)	3% (2)	1% (1)	4% (3)	0% (0)	1% (1)	<b>3.38</b>
Strong Security	19% (13)	16% (11)	<b>22% (15)</b>	18% (12)	9% (6)	3% (2)	3% (2)	4% (3)	0% (0)	3% (2)	3% (2)	<b>3.68</b>
Fine Granularity (e.g. assigning resources to classes)	0% (0)	6% (4)	1% (1)	7% (5)	13% (9)	13% (9)	9% (6)	10% (7)	10% (7)	6% (4)	<b>25% (17)</b>	<b>7.51</b>
Flexibility to Cope with Changes & Additions	3% (2)	0% (0)	12% (8)	10% (7)	16% (11)	<b>22% (15)</b>	10% (7)	9% (6)	6% (4)	10% (7)	1% (1)	<b>6.07</b>
Cross Platform Functionality	1% (1)	1% (1)	6% (4)	1% (1)	7% (5)	16% (11)	<b>21% (14)</b>	6% (4)	16% (11)	9% (6)	15% (10)	<b>7.49</b>
User Privacy	1% (1)	4% (3)	6% (4)	10% (7)	9% (6)	13% (9)	13% (9)	<b>20% (14)</b>	9% (6)	13% (9)	1% (1)	<b>6.68</b>
Individual User Accountability	4% (3)	6% (4)	3% (2)	9% (6)	<b>16% (11)</b>	9% (6)	9% (6)	10% (7)	<b>16% (11)</b>	14% (10)	4% (3)	<b>6.70</b>
Collection of Management Data	1% (1)	0% (0)	3% (2)	12% (8)	10% (7)	4% (3)	15% (10)	<b>16% (11)</b>	<b>16% (11)</b>	<b>16% (11)</b>	6% (4)	<b>7.40</b>
Facilities for Users with Affiliations to Multiple Institutions	4% (3)	0% (0)	1% (1)	1% (1)	4% (3)	6% (4)	4% (3)	9% (6)	15% (10)	18% (12)	<b>37% (25)</b>	<b>8.87</b>
<b>Total Respondents</b>												<b>70</b>

# Appendix G

## Comparative Analysis: Table

---



## Appendix G – Comparative Analysis

	<b>Athens: Classic Accounts</b>	<b>Athens: Personal Accounts</b>	<b>Athens: AthensDA</b>	<b>Shibboleth</b>
<b>Feasibility &amp; Deployability</b>	<ul style="list-style-type: none"> <li>+ feasible</li> <li>+ easy to administer</li> <li>+ easy to deploy</li> <li>- not appropriate for distance users</li> </ul>	<ul style="list-style-type: none"> <li>+ feasible</li> <li>+ easy to deploy</li> <li>- can involve a lot of work to administer</li> </ul>	<ul style="list-style-type: none"> <li>+ feasible</li> <li>+ easy to administer</li> <li>- deployment can be technically challenging</li> </ul>	<ul style="list-style-type: none"> <li>+ feasible</li> <li>- resource access administration potentially complex</li> <li>- challenging to deploy</li> </ul>
<b>Authentication Strength</b>	<ul style="list-style-type: none"> <li>+ secure hosting</li> <li>- shared account</li> </ul>	<ul style="list-style-type: none"> <li>+ secure hosting</li> <li>+ personal account</li> <li>- not always anonymous</li> </ul>	<ul style="list-style-type: none"> <li>+ secure hosting</li> <li>+ linked to existing institutional account</li> </ul>	<ul style="list-style-type: none"> <li>+ secure hosting</li> <li>+ linked to existing institutional account</li> <li>+ SAML protocol</li> </ul>
<b>Granularity &amp; Extensibility</b>	<ul style="list-style-type: none"> <li>+ additions easy to implement</li> <li>+ some granular</li> </ul>	<ul style="list-style-type: none"> <li>+ additions easy to implement</li> <li>+ some granular control using groups or permissions sets</li> </ul>	<ul style="list-style-type: none"> <li>+ additions easy to implement</li> <li>+ some granular control using permissions sets</li> </ul>	<ul style="list-style-type: none"> <li>+ additions easy to implement</li> <li>+ fine grained access control</li> <li>- heavy administrative load to control access</li> </ul>

	<b>Athens: Classic Accounts</b>	<b>Athens: Personal Accounts</b>	<b>Athens: AthensDA</b>	<b>Shibboleth</b>
<b>Cross-Protocol Flexibility</b>	- restricted to web - proprietary components	- restricted to web - proprietary components	- restricted to web - proprietary components	+ open source + standards based + not limited to web
<b>Privacy Considerations</b>	+ individuals not identified	+ potential for pseudonymous access  - potential for identified access	+ pseudonymous	+ pseudonymous + attribute release policies
<b>Accountability</b>	- limited accountability owing to shared status	+ high level of accountability  + easy access by Administrator	+ high level of accountability  - reliant on IT Services for access to logs	+ some information held by service host - dependent on setup - no log review tools
<b>Collection of Management Data</b>	+ collection of data at resource level  - no collection of user data beyond that for shared account	+ collection of data at resource level  + collection of data at user level	+ collection of data at resource level  + collection of data at user level	- not an integral component

+ = positive comment

- = negative comment

# Appendix H

## Respondent Comments

---

## Appendix H – Respondent Comments

We are actively investigating Shibb as we know Athens DA has a shorter life than originally expected. Also we are an institution which could not afford to pay for the access mechanism under current budgets.

We have just recently moved to AthensDA and one of the pluses is that users do not need a separate Athens username/password to access Athens authenticated resources but can use their University network login details. One of the drawbacks is that we have a small group of users who do not have University logins so they will have to continue with the old classic Athens accounts.

Notwithstanding my selections in the survey, the ease of transition between access management systems is key. If an institution has something that seems to work it is far harder to justify changing it all.

We will be going to Shibboleth soon but have not got it set up yet, I'm not involved in that but I am looking forward to it reducing my Athens work - all those endless 'I've forgotten my password' enquiries.

Although I have said that we haven't used Shibboleth we are in the early stages of setting up access as second round early adopters

This is no firm information on what will happen to Athens/EduserV after July 2008 so Shibboleth is tentatively being looked into. I do not believe Shibboleth will be easier to use than AthensDA and it will definitely NOT be free (which some people believe...).

We are a very small HE college with just 400 students. We subsequently have a small library and a very small IT dept. Our concerns with moving away from Classic Athens are generally based upon not having the staff resources to introduce and maintain other access management systems. So even though we like the look of Athens DA & Shibboleth, I think they are more suited to larger institutions.

The main benefits to using Athens are the ease of set-up and maintenance. Many service providers use Athens as a means of authentication and this means that any changes will have a big impact, especially on smaller institutions who may not have resources to deal with changes. The main drawbacks are lack of security, it's not very difficult for users to by-pass systems.

When I took on the role of Athens Administrator it was not explained to me fully how much work there was involved. (I am an Administrator for a large area). There are problems at times with Athens registration, as Athens applicants complete the online registration form incorrectly.

We currently use personal accounts for managing ATHENS access, but hope to move over to Shibboleth by 2008. We hope this will be easier for our users, and more secure. Currently it can be confusing for users who are affiliated to more than one institution, that the resources they need are accessed via two or more ATHENS logins. We often have problems with our Health students trying to access NHS resources via their university login and vice versa.

I am an NHS administrator for ATHENS and seem only to be aware of implications for my institution. I don't think that (in general) NHS people fulfilling this role know much about the background, the technicalities, or the possibilities for future development.... but Athens works quite well for us at the moment.

Please note that we will be introducing AthensDA for the new academic year.

Hi Ian Please feel free to get in touch if you want to go into a bit more detail we are implementing AthensDA in Sept thanks

Overall ATHENS provides an effective if rather 'clunky' solution to the problems of electronic access management. Shibboleth would be an even better one but as a smallish institution we will probably have to wait to implement the latter. We are quite happy with ATHENS in the interim. Greater problems/gripes are probably expressed with actual access to full text content and multiple interfaces/searches rather than the method of access.

[end]