The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0033-0337.htm

Authentication and authorisation infrastructure for the mobility of users of academic libraries

An overview of developments

Emil Hudomalj
Institute of Biomedical Informatics, Faculty of Medicine, University of Ljubljana, Slovenia, and
Avgust Jauk
Academic and Research Network of Slovenia, Ljubljana, Slovenia

Received 25 March 2005
Revised 3 October 2005
Accepted 19 October 2005

Abstract

Purpose – To give an overview of the current state and trends in authentication and authorisation in satisfying academic library users' mobility and instant access to digital information resources, and to propose that libraries strongly support efforts to establish a global authentication and authorisation infrastructure.

Design/methodology/approach – An overview of some national projects towards such an infrastructure for public institutions, including libraries, is provided.

Findings – There are many projects working towards such an infrastructure, but no single widely accepted authentication and authorisation infrastructure exists yet. A global authentication and authorisation infrastructure will enable users to use a single username and a password for all local and remote library services. It will consist of interconnected authentication/authorisation servers, where each institution will be responsible for a local user database.

Research limitations/implications – The list of projects towards global authentication and authorisation infrastructure is not complete. Projects are not described in detail.

Practical implications – Libraries will have to join efforts towards a global authentication and authorisation infrastructure and to integrate this into their applications. That way, they will improve services for their users who are remote from their home institutions, enable users to access new services faster, lessen user frustration with forgotten passwords, reduce time spent on administrative tasks and also reduce the burden of password management and enable security improvements.

Originality/value – This paper fulfils an identified need to speed up the development of a global authentication and authorisation infrastructure.

Keywords Mobile communication systems, Academic libraries, Research libraries, Electronic media

Paper type Technical paper

1. Introduction

Traditionally, libraries have tried to provide information to their users in a friendly and easy way. To satisfy this common goal, during the 1980s and 1990s libraries had to

The authors would like to thank Gaj Vidmar from the Institute of Biomedical Informatics in Ljubljana for his valuable collaboration, and Anamarija Rožić from the Central Medical Library in Ljubljana for her suggestions during the preparation of this paper. They are also grateful to the editor and two anonymous referees for valuable comments.

Program: electronic library and information systems
Vol. 40 No. 1, 2006
pp. 63-73
© Emerald Group Publishing Limited
0033-0337
DOI 10.1108/00330330610646816

face many challenges, such as implementing their own OPAC and other databases, installing CD-ROM databases in local networks, providing access to remote online databases and journals, implementing interlibrary lending services over e-mail, and building websites and portals (e.g. Campbell, 2003). Nowadays, the internet is an integral part of library services (e.g. Bertot, 2003).

In academic environments, professors, researchers and students wish to use network services from various campus locations, as well as from home and while travelling around the world. To support mobility, many libraries lend laptop computers to their users (Vaughan, 2002), and many users also have their own notebook computer and a mobile phone. It is necessary to ensure that a specific user has the necessary identification (authentication), and based on this (and possibly other information), it will be necessary to determine what privileges the user has in order to be able to use the digital sources and services (authorisation). However, while using services in different places, many users may have difficulties, such as inability to access locally held databases at the university, remembering different passwords for local as well as remote services (e.g. access to e-journals). McLean (2000) described these challenges from the library's point of view and outlined solutions being investigated at that time at Maquarie University in Australia.

2. Some existing authentication and authorisation (AA) solutions

Solving the AA challenge with passwords and usernames has been a well-used approach. However, password management is one of the most time-consuming activities for helpdesk staff in many institutions. Clark (2003) reports that 30 percent of calls to helpdesks are from users who have forgotten their passwords or whose passwords have expired. Users are discouraged from storing their passwords on their system and are also encouraged, by system managers, to change their passwords regularly and not to reuse passwords so as to conform to international standards for information security within an institution (British Standards Institution, 2000, 2002). For these reasons, many institutions have implemented central password management applications (such as Microsoft's Active Directory), or automatic password management applications as described by Clark (2003). These are rather expensive solutions and can usually solve problems only within an institution – they do not provide a solution for libraries that have remote users accessing remote services.

One solution adopted to overcome use of passwords is to check the IP (internet protocol) address of the user, although this has several drawbacks, as outlined by McLean (2000). First of all, it only assures that the institution using the IP addresses in question has the right to use the resource, and not the actual user using the computer. Also, there are well-known methods for "spoofing" IP addresses. IP address checking also prevents organisations and individual users from using internet service providers (ISPs) that provide IP addresses dynamically, i.e. per connection (this is often used for dial-in, wireless access (Wi-Fi) or asymmetric digital subscriber Line (ADSL)), or ISPs that use the network address translation (NAT) mechanism to hide many users behind a single IP address, often used to provide access via mobile phones.

User-level AA is the better solution. The most widely adopted method for user authentication is based on usernames and passwords. This has the drawback of users having to remember a new password for each of the services they are accessing. One solution is the provision of an AA infrastructure that would provide users with means of using a single username and password for seamless and location-independent access to the network, as well as to application services.

Several research and education communities have already initiated projects to provide such services to public institutions, including libraries. Examples include:

- *Athens* (see www.athens.ac.uk/) has been in operation since 1996 and has firmly established itself as the *de facto* standard for secure access management to web-based services for UK higher education (HE) and further education (FE) as well as the health sector. It provides users with a single sign-on to enable access to digital information services within the UK as well as overseas. Athens holds three million user accounts from over 2,000 organisations and controls access to 260 services and is currently the service contracted by the Joint Information Systems Committee (JISC) for the provision of authentication services for UK HE and FE.
- *PAPI* (see http://papi.rediris.es/) was developed by the Spanish national research and education network, RedIRIS, as a solution to the user authentication problems identified by Spanish library consortia and content providers. They were looking for a mechanism that would replace user authentication based on the IP addresses, keep authentication as an issue local to the organisation the user belongs to, while leaving the information providers full control over the resources they offer.
- *Shibboleth* (see http://shibboleth.internet2.edu/) is a project of the Internet2 Middleware Architecture Committee for Education (MACE) (Paschoud, 2004). Internet2 is a consortium of 207 US universities, working in partnership with industry and government, to develop and deploy advanced network applications and technologies and is involved in developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. Shibboleth specifies a mechanism to enable access control to web resources, utilising SAML (Security Assertion Mark-up Language) for the exchange of attribute and authentication information, with particular emphasis on protecting user privacy. Shibboleth is in the process of being adopted in Australia, Finland and Switzerland. In the UK in 2005, the JISC is funding 15 projects exploring different aspects of moving from Athens to Shibboleth.

There are also other national projects, such as A-Select in The Netherlands (see http://a-select.surfnet.nl/), FEIDE in Norway (see www.feide.no/index.en.html), and SWITCH-AAI in Switzerland (see www.switch.ch/aai/).

It will be a significant management challenge to deploy a real global AA infrastructure in a consistent and coherent way across the educational and research community. Perhaps the most important initiative towards this goal has been started within the project Study into European Research and Education Networking as Targeted by eEurope (SERENATE) (see www.serenate.org/). SERENATE, which ran between 2002 and 2003, and was funded by the European Commission, comprised a series of strategic studies into the future of research and education networking in Europe over the next five to ten years. It stressed the importance of co-ordination of national research and education networks and those responsible for IT services at the national and campus level in several areas, especially the co-ordinated access to content, such as distance-education material and commercial databases. Within the project some recommendations for the European Commission were given, and one of the most important ones was to establish an AA infrastructure across Europe and globally.

To summarise, mechanisms currently used by the majority of libraries either do not support mobility of users, are quite cumbersome to use, or are limited in scope. Therefore, the development and adoption of new, standardised mechanisms is needed.

3. Technical background and requirements

Technology improvements during the last few years have brought new ways of connecting users to the digital information sources provided by academic libraries. Users can dial-in via the phone network, use different broadband technologies such as ADSL and cable modems, use Wi-Fi technology to connect via wireless links, or use mobile telephony services.

In an attempt to bring together those working on national mobility and AA infrastructure projects in different countries, the Trans-European Research and Education Networking Association (TERENA) has funded various task forces (typically with a life span of 18-24 months) to investigate specific aspects. Examples include:

- Task Force on Authorisation and Authentication Co-ordination in Europe – TF-AACE (see www.terena.nl/tech/task-forces/tf-aace/) (TERENA, 2004); and
- Initiative to co-ordinate mobility related activity among National Research and Education networks (NRENs) in Europe – TF-Mobility (see www.terena.nl/tech/task-forces/tf-mobility/) (Sankar and Wierenga, 2004).

Since the AA infrastructure is being established as a basic middleware infrastructure rather than a set of applications for a certain purpose, mechanisms providing interoperability between different solutions are being developed. This work is being undertaken in another TERENA task force – the European Middleware Co-ordination and Collaboration (TF-EMC2) (see www.terena.nl/tech/task-forces/tf-emc2/). The work started in late 2004 and is expected to carry on for two years. The aims of the task force are:

- to provide a forum for exchanging experiences and knowledge;
- to promote the development and testing of innovative middleware technologies;
- to promote the use of common standards and procedures in the middleware infrastructures;
- to promote the actual use of middleware infrastructures at the campuses; and
- to liaise with other middleware activities at international level, such as the Global Grid Forum (GGF) and Internet2.

Although many different AA infrastructure architectures exist, there are no signs at present that a single solution will prevail. The requirements that an AA infrastructure has to fulfil in order to be accepted by users, administrators and service providers include:

- Security must be maintained for all partners in the process. In addition to protection against eavesdropping, data manipulation and session hijacking, appropriate levels of user privacy should be maintained as well.
- Accounting and logging functionality must be provided to enable charging where needed and to facilitate abuse tracking.
- The infrastructure should be based on open standard mechanisms to facilitate interconnection.
- The infrastructure has to be scalable.
- Administrative overheads must be minimised. User administration should be limited to their home organisations.
- Usability must be good for all the platforms in use, different operating systems and applications have to be supported and preferably no installation of new software should be required on the client side.

In addition to the technical requirements, a written policy is required – a set of rules defining behaviour and responsibility of all participating parties, i.e. end users, their home organisations, intermediaries, and service providers. Such a policy has to adhere to relevant national as well as international legislation, especially the data protection and privacy laws.

The ultimate goal is to have a solution that would provide single sign-on (SSO) to the network as well as to the applications. With such mechanisms in place, users will have to login only once to get access to the network and also to the application services. As an intermediary step, two separate SSO solutions are being developed:

- one for login for network access (i.e. eduroam, as described later); and
- one for access to applications/services (i.e. Athens, Shibboleth, A-Select, PAPI, etc).

In principle, it should be possible to build one general infrastructure, but since the application sign-on requires IP connectivity (which is not available at the time of network login), a two-phase sign-on would still be necessary. The integration of both into an SSO might require changes to the network access devices and therefore presents a more ambitious goal.

Lacking a standard solution for sign-on accepted by everybody, mechanisms for providing interoperability are needed, i.e. some kind of gateways interconnecting existing AA infrastructures. Due to the large number of different AA infrastructure architectures already in use, the development of gateways between each and every AA infrastructure solution is not feasible since too many gateways would have to be developed and maintained. That problem is being addressed by the GÉANT2 JRA5 project. GÉANT2 is a pan-European research and education network linking 34 countries through 30 NRENs. The project within which GÉANT2 is funded began officially on 1 September 2004, and will run for four years (see www.geant2.net/).

The JRA5 project will develop a pilot infrastructure for AA in the form of a superstructure capable of integrating existing and future national and organisational AA infrastructures into a federation of autonomous AA infrastructures. In its final form it will serve as a unified SSO solution to the network as well as to the applications.

Every local AA infrastructure will have to build only one gateway, called the Local Federation Connector (LFC), connecting the AA infrastructure to the superstructure.

One example of such federated AA infrastructures, although with the scope limited to controlling access to the network resources, has been built as a pilot roaming authentication service for higher education and research – eduroam (see www.eduroam.org/). Eduroam resulted from a proof of concept test undertaken within TF-Mobility and involving NRENs in Croatia, Finland, The Netherlands, Portugal and the UK. By mid-2005 some 13 other European countries were also connected to eduroam, as well as Australia.

The eduroam infrastructure is based on a hierarchy of Remote Authentication Dial In User Service (RADIUS) servers enabling international roaming of users from the education and research community (see www.ietf.org/rfc/rfc2865.txt). The hierarchy consists of organisation level, national level and international level (root) RADIUS servers. It is used during the user authentication process to find the RADIUS server of the organisation to which the user belongs. Credentials needed for user authentication (usernames, passwords, etc.) are maintained by home organisations. They are normally stored in the Lightweight Directory Access Protocol (LDAP) directories. Although other storage mechanisms are also supported by RADIUS servers, LDAP has certain advantages. Amongst others, it can be directly used for authentication and authorisation by computer operating systems and web-based applications through Pluggable Authentication Modules (PAM).

The infrastructure used in eduroam provides authentication mechanisms that can be used to control access to the wireless networks – as specified by the Institute of Electrical and Electronic Engineers (IEEE) 802.11 Working Group on Standards for Wireless Local Area Networks (see http://grouper.ieee.org/groups/802/11/). Also, the eduroam infrastructure provides authentication mechanisms that can be used by switched wired networks where ports on switches are protected by IEEE 802.1X port-based network access control mechanisms. In addition to user authentication, RADIUS servers local to the network access devices can be used to provide limited authorisation mechanisms. For example, if the 802.1X port-based security mechanism is used, an appropriate Virtual Local Area Network (VLAN) defined by the local authorisation policy can be assigned to the user.

The infrastructure currently used for eduroam does not provide a complex user authorisation mechanism and is therefore not suitable for roaming access to applications. There are several ways of overcoming this drawback. Authentication mechanisms could be provided by incorporating RADIUS clients into applications or by setting up proxies/gateways to the eduroam RADIUS infrastructure. Since current eduroam service prevents malicious resource owners from stealing user's authentication credentials, it is important to keep this property in case RADIUS infrastructure is used also for roaming access to applications.

In order to provide complex authorisation mechanisms, more work will have to be done. An example on how to extend the RADIUS infrastructure with authorisation capabilities is given by the UK JISC project LICHEN – Location Independent Collaboration in Higher Education Networks (November 2004-October 2005; see www.iam.ecs.soton.ac.uk/projects/LICHEN.html).

As a step toward implementing single sign-on, the GÉANT2 JRA5 project will further develop the eduroam concept under the name eduroam-ng, which is supposed to support both network-level and application-level authentication and at a later stage integrate it with a more general AA superstructure.

4. Authentication and authorisation infrastructure from a user point of view

Nearly every application or service that has to authorise users could benefit from an AA infrastructure, especially those available to users from different institutions and those whose users change often. From the user perspective, services can be grouped into home services, local services, and remote services. Below, there are some examples of how the AA infrastructure could be seen from a user point of view in a very simplified manner. We use simplified examples of how eduroam RADIUS infrastructure could be used for such purposes.

4.1 Home services

These are services provided by an institution primarily for its own staff, students and so on. Such services include e-mail and access to various databases. An example is presented in Figure 1. When a user from institution A tries to connect to the service, they are usually asked for a username and a password. The service can use RADIUS and its database to check the credentials. If the operation is successful, the user is granted access to a service. More detailed rights can be assigned to the user depending on values in the database and settings of the service (i.e. for e-mail, a user can or cannot be allowed to set a forwarding address over an e-mail client). Actually, this is the standard procedure used by many applications nowadays, except that most of them use proprietary databases for storing usernames and passwords (e.g. Microsoft's Active Directory).

4.2 Local services

These are defined as services provided by an institution not only to local users (staff, students), but also to guests. Among these services, physical access to the network, connection to printers, disks, etc. could be included. An example is presented in Figure 2. A user can access the network by a wired connection or by wireless. As soon as the user tries to connect to the network (before a service is reached), the authenticator asks the user for username and password. The authenticator (as in the previous example) uses RADIUS and its database to check the credentials. If a user is registered at institution A, the same procedure is used as for home services. For users from other institutions (i.e. B in Figure 2) a similar procedure is performed, except that the password is checked at the remote RADIUS server at institution B reached via the proxy RADIUS hierarchy. After the authorisation process, the user is connected to a VLAN, depending on user's rights in the local database and (for visiting users) the remote database. There can be several VLANs available: a special VLAN for internet connection, special VLANs for guests, students, or employees (maybe a library's administrative VLAN). For visiting users, the assignment of a VLAN is based on the rights in local and remote databases and may be also on the access method. As a member of a VLAN, the user gets the possibility to use services available on that VLAN (before use, the user has to authenticate again). The solution in this example is also important from a security viewpoint. It enables guest users to use certain local

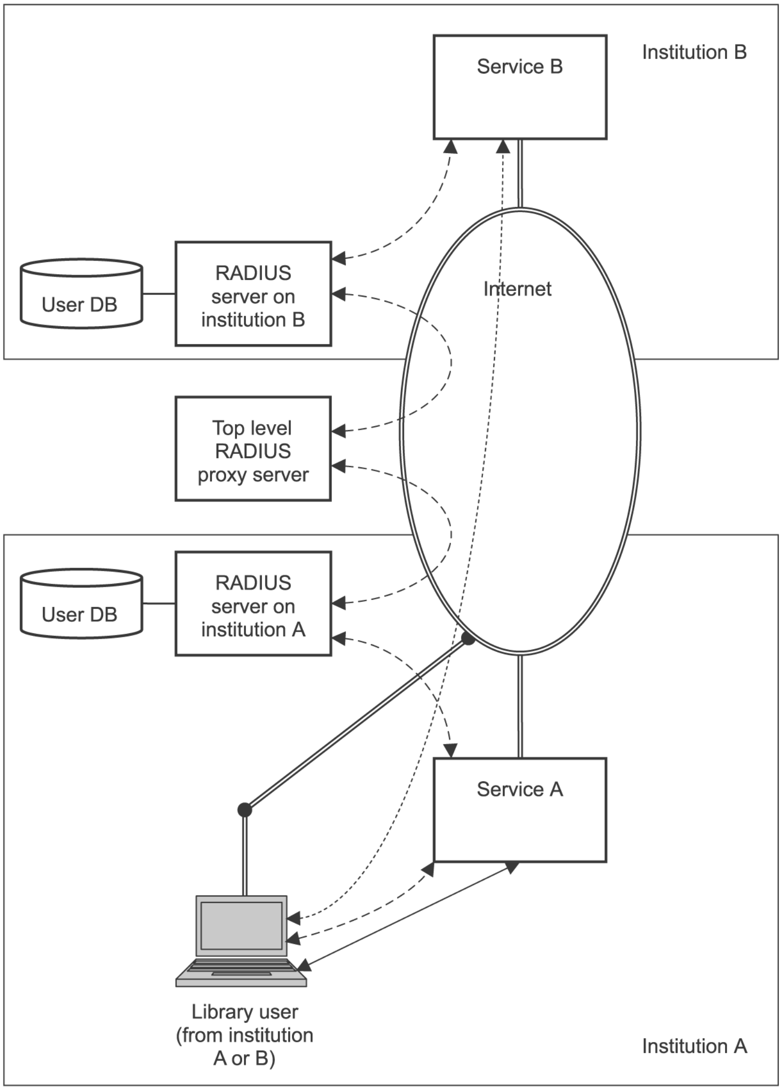
Service B
Institution B
User DB
RADIUS server on institution B
Internet
Top level RADIUS proxy server
User DB
RADIUS server on institution A
Service A
Library user (from institution A or B)
Institution A

Figure 1.
An example of using an AA infrastructure for home (solid line) and remote service (dotted line). Dashed line indicates the flow of authentication and authorisation data

services over the same infrastructure as local users, while at the same time preventing them from reaching some secure services like administration databases.

4.3 Remote services

These are defined as services that are provided by a distant institution, including commercial bodies such as e-journal publishers and bibliographic database providers. In Figure 1, such a service is provided by institution B. When users from institution A reach such a service, their passwords are checked in the database of the RADIUS server at institution A, which is reached over the RADIUS server at institution B and

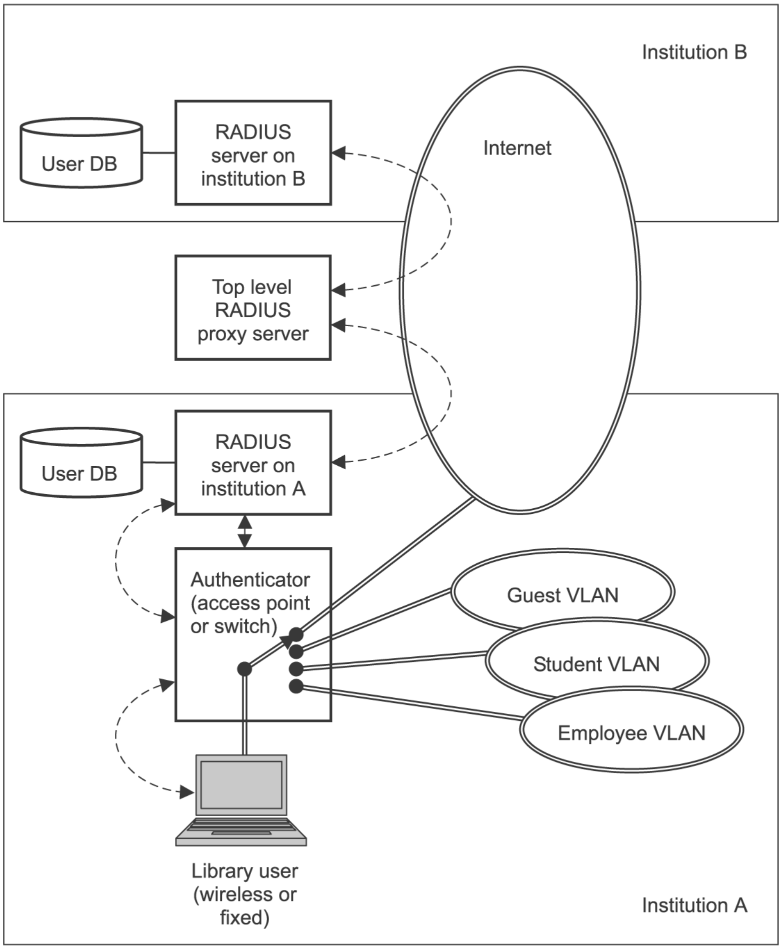
Institution B
User DB
RADIUS server on institution B
Internet
Top level RADIUS proxy server
User DB
RADIUS server on institution A
Authenticator (access point or switch)
Guest VLAN
Student VLAN
Employee VLAN
Library user (wireless or fixed)
Institution A

Figure 2.
An example of using AA infrastructure for access control of a library user. The dashed line indicates the flow of authentication and authorisation data

the proxy server. Of course, the procedure will be the same if a user from institution A is at some time located at institution B or elsewhere where the AA infrastructure has been set up.

5. Discussion and conclusions

An AA infrastructure can improve the usability of the services offered by libraries to their users. We believe that users will strongly appreciate the possibility of using one password for many local and remote applications. The importance of this feature will grow with the number of services offered, and in a few years it could be a crucial requirement of many users, at least those who use many services. Libraries that implement the AA infrastructure could become the preferred choice for these users. The development of such infrastructure is the key also for enlarging the information services market through offering cost effective and secure information access (McLean, 2000).

From the users' perspective, an AA infrastructure will improve their mobility, enable them to access new digital information sources and services faster, lessen frustration with forgotten passwords, and lessen the time spent on administrative tasks at institutions visited. From the institutions' point of view, we can expect less time spent on password administration and more possibilities for security improvements. One such security feature would be the requirement to change passwords on a monthly basis or so as suggested by the British and international standard (British Standards Institution, 2000, 2002); due to user resistance, this is frequently not obeyed. Another security benefit would be the fact that users (hopefully) will not lend their passwords to their friends to access some non-personal information, because the same password will also be used to access personal information, such as e-mail. In the future, the same infrastructure could use other types of user credentials, like public keys for asymmetric cryptography applications.

The need for an AA infrastructure is pressing, not only in the educational and research environment, but also in the commercial environment. Two of the most widely published initiatives are Passport (see www.passport.net) and Liberty Alliance (see www.projectliberty.org/). While Passport seems to be losing support due to its proprietary nature, Liberty Alliance is gaining momentum. Since most libraries have some users from outside the educational and academic environment, they will also have to provide support for commercial AA infrastructures.

It will take a lot of time and effort to establish an AA infrastructure on a broad scale, but this does not have to be an excuse to avoid planning such activities. Therefore, we propose that first a clear list with home and local services is made, then services which will be offered remotely would be included. Second, within the home institution a pilot project could be established. Not much more technical work would be required afterwards to connect some other institutions to build an "island" AA infrastructure, which could afterwards be merged with other islands. But we would like to emphasise that a significant amount of work should be devoted to collaboration and setting up new standards, or at least their adoption at an appropriate time. Some institutions which are responsible for academic networking play a major role in this field, so probably they are the best place to get further information about standardisation activities, pilot projects, organisation of projects and maybe also about funding. It seems that the GÉANT2 JRA5 project is one of the most promising activities towards a global AA infrastructure that will provide SSO both for network access and for access to applications.

Altogether, some of the appropriate technologies are already developed or are being developed and, beside technical changes in infrastructure, considerable management effort and especially co-operation among institutions will be required to offer such services to users. Libraries have historically been early adopters of technology (e.g. Logue, 2003), so another step in this direction should be seen as a natural development of services for the users.

References

Bertot, J.C. (2003), "World libraries on the information superhighway: Internet-based library services", *Library Trends*, Vol. 52 No. 2, pp. 209-27.

British Standards Institution (2000), *Information Technology – Code of Practice for Information Security Management: British Standard*, BS ISO/IEC 17799:2000, BS 7799-1:2000, British Standards Institution, London.

British Standards Institution (2002), *Information Security Management Systems – Specification with Guidance for Use: British Standard*, BS 7799-2:2002, British Standards Institution, London.

Campbell, J.D. (2003), "Access in a networked world: scholars portal in context", *Library Trends*, Vol. 52 No. 2, pp. 247-55.

Clark, E. (2003), "Making peace with passwords", *Network Magazine*, (re-titled *IT Architect*), June, pp. 42-6, available at: www.itarchitect.com/shared/article/showArticle.jhtml?articleId=15201403

Logue, S. (2003), "Guest editorial: the changing role of libraries in instructional support", *Information Technology and Libraries*, Vol. 22 No. 2, pp. 2-3.

McLean, N. (2000), "Matching people and information resources: authentication, authorisation and access management", *Program*, Vol. 34 No. 3, pp. 239-55.

Paschoud, J. (2004), "Everything I always wanted to know about Shibboleth . . . but was afraid to ask Alan Robiette", available at: http://hdl.handle.net/1988/58

Sankar, J. and Wierenga, K. (2004), "TF-Mobility: inter-NREN roaming", *TERENA Task Mobility (TF-MOBILITY) – Final Report*, available at: www.terena.nl/tech/task-forces/tf-mobility/Deliverables/TF-MobilityfinalReport.pdf

TERENA (2004), *TERENA Task Force on Authentication and Authorisation Coordination in Europe (TF-AACE) – Final Report*, available at www.terena.nl/tech/task-forces/tf-aace/Del/TFAACE-FinalReportv-2.pdf

Vaughan, J. and Burnes, B. (2002), "Bringing them in and checking them out: laptop use in the modern academic library", *Information Technology and Libraries*, Vol. 21 No. 2, pp. 52-62.

Corresponding author
Emil Hudomalj can be contacted at: Emil.Hudomalj@mf.uni.lj.si