Security and online content management – balancing access and security

Raj Saxena
Manager, Information Systems and Resources
Frank Lowy Library
Australian Graduate School of Management
rajs@agsm.edu.au

Abstract:
This paper describes the implementation, benefits and implications of various security and access management systems employed by Australian Graduate School of Management and its Electronic Library. In particular, the paper discusses the automated access management process of eTrust SSO (Single Sign-On) product and its integration levels with the Library's ILMS.

Introduction

In today’s world, identification, authentication and authorisation are usually done with an array of user names and passwords. In this environment, the regulation of user access to networked electronic resources is becoming an increasing problem for libraries and their communities. With the advent of Web-based online products that can exist anywhere in the world or even be scattered around campuses and behind firewalls, libraries are challenged either to develop homegrown solutions or implement sophisticated softwares.

While these solutions may work well for a library, they may not take into account the many issues that should be considered when implementing an access management system. The key constituents in the scholarly communication process, the online content providers, the libraries licensing the electronic resources, and the user community, all have specific interests that need to be balanced in any authentication solution.

This paper will describe the implementation, benefits and implications of various security and access management systems employed by Australian Graduate School of Management (AGSM) and its Electronic Library.

AGSM Background

The AGSM was established as a faculty of the University of New South Wales (UNSW) admitting its first MBA class in 1977. In 1999 it became a school of the University of New South Wales and the University of Sydney.

Today AGSM is ranked as one of the top business schools in Australia and is consistently recognised among the top ten business school in Asia-Pacific.[1,2] In 2002, the AGSM’s 25th anniversary year, it became the first business school in Australia to receive international accreditation from the Association to Advance Collegiate Schools of Business[3] (AACSB), an honour granted to institutions which fulfil the highest standards in curriculum, faculty, research and teaching.

The AGSM’s dedicated post-graduate campus at the UNSW’s Kensington campus has now opened an office in Hong Kong and further expanded in 2002 with a Sydney CBD campus. Wide ranges of research-driven programs are offered in these campuses that make up the student population of AGSM. Programs are also taught face to face simultaneously in 11 locations in 6 Australian capital cities. The programs include a full-time MBA program that is generally completed within 18 months. This also includes an exchange program with 31 top business schools worldwide. The MBA Executive program has various entry points (e.g. Graduate Certificate in Management and Graduate Certificate in Change Management) and students can finish in as little as 2.5 years, or take as long as 7 years. The AGSM’s structured PhD program also offers a world-class training in research, which attracts students from a wide variety of disciplinary backgrounds ranging from politics, mathematics, the sciences and the arts. The Executive Programs and the Corporate Education programs have the largest product suite in Australia that provides open enrolment and customized programs.

Together, this diversity in student population and an increase in the number of courses being offered in flexible delivery mode, demand a very efficient and effective management of online resources and applications.

Access Management Issues

With the advent of the Internet, online users have come to expect immediate and unencumbered access to information. It is unrealistic to expect students, many of whom are balancing part-time school schedules with full-time work schedules, to wait for days to gain access to research resources.

As AGSM has expanded its products and services online, it has faced one of its biggest challenges: providing users and customers with a simple and secure access management system. In the past, the requirement of multiple login procedures was tolerated and some even considered it stringent security. Today, such a requirement can act as a deterrent. Users become easily frustrated with multiple, complicated logins, and the more passwords they must remember, the more likely it is that the organisation's online security will be compromised.

Providing a Solution

AGSM has addressed these concerns by investing in a product developed by Computer Associates (CA) called *eTrust Single Sign-On*[4] (eTrust SSO). SSO provides the AGSM community with easy access to their multiple platforms and applications while ensuring that data and applications remain secure.

The central function of this implementation is the single authentication (single username and single password). This not only makes life easier for users of online application and resources but also enhances password management by giving help desk or system administrators a consolidated view of all users accounts.

User Authentication and Authorisation

Authentication is the process by which a security system challenges prospective users to identify and confirm their identities (Lynch 1998). It is the process where a user supplies some kind of secret information (e.g. a password) to prove that he or she should be allowed to use an online identifier. It answers the question: *Do you have the right to use a particular User ID*?

Authorisation, on the other hand, is the process of determining whether a User ID is able to access a resource or perform a given transaction (Lynch 1998). It answers the question: *What can or can’t you have access to*?

Following through on Lynch’s (1998) use of terminology, the term “access management” is used to indicate a methodology that incorporates both aspects of authentication and authorisation.

With the implementation of SSO at AGSM, access management is administered globally, enabling immediate changes for SSO users and applications. Changes can be applied across the entire AGSM user population, or they can be selectively applied to a group or an individual user.

The eTrust SSO provides a proprietary mechanism for initial user authentication. This authentication method is inherent to eTrust SSO and does not require any additional components or products.

Users authenticate themselves once and are presented with their customized applications. This simple login process has enabled AGSM to move from password-based logins to strong authentication method without visibly impacting the user login process.

What is SSO?

Computer Associates (2000) defines SSO as a mechanism whereby a single action of user authentication and authorisation can permit a user to access all computers and systems where that user has access permission at their designated level, without the need to enter multiple passwords. SSO provides users with single sign-on, authentication and authorisation services to all authorized Web applications and Web resources. After the first login, the SSO product handles the login process to other Web pages and applications. Once users login to an SSO domain they can access secured resources within that domain without being challenged again.

Although the process of logging on to a system seems simple, that is to enter your user identification name (user ID) and then your password, it actually sets several actions in motion. The first, authentication, occurs when the system verifies that the entity (person or program) logging on is the entity associated with that user ID, usually by matching the password with the user ID (CA 2000).

Authorisation comes after the user is authenticated and tries to access the networked resources. The user may be authorised to view files but not to delete or modify them. A typical example will be a library staff member looking at student details in a student database. The SSO system responds to unauthorised requests with an error message and responds to authorized requests by allowing the desired access. The actual authorisation happens immediately after the authentication, with the user getting a list of authorized resources.

At its simplest, SSO is implemented so that each user has an account with an authentication server, which stores all user IDs, passwords and other account information. The server authenticates the user once and then passes user ID and password information to other domains as needed.

For the end users, this means only one password to remember and update, and one set of password rules. For the administrators, this means a single common registry of user information management and security infrastructure. Centralizing authentication and authorisation with SSO not only helps the user, but it also removes administrative problems by radically lowering the number of requests for password help and allowing for quick and easy removal of privileges for a non-current student or a terminated employee. Instead of tracking down all the systems and resources to which the user might have had access, administrators can simply remove the user's SSO account.

On the downside, an SSO can represent a single point of failure for network security. It may also take a bit of work to establish access to all network resources in an organisation. However, IT staff at AGSM have regarded the benefits as worth the additional workload.

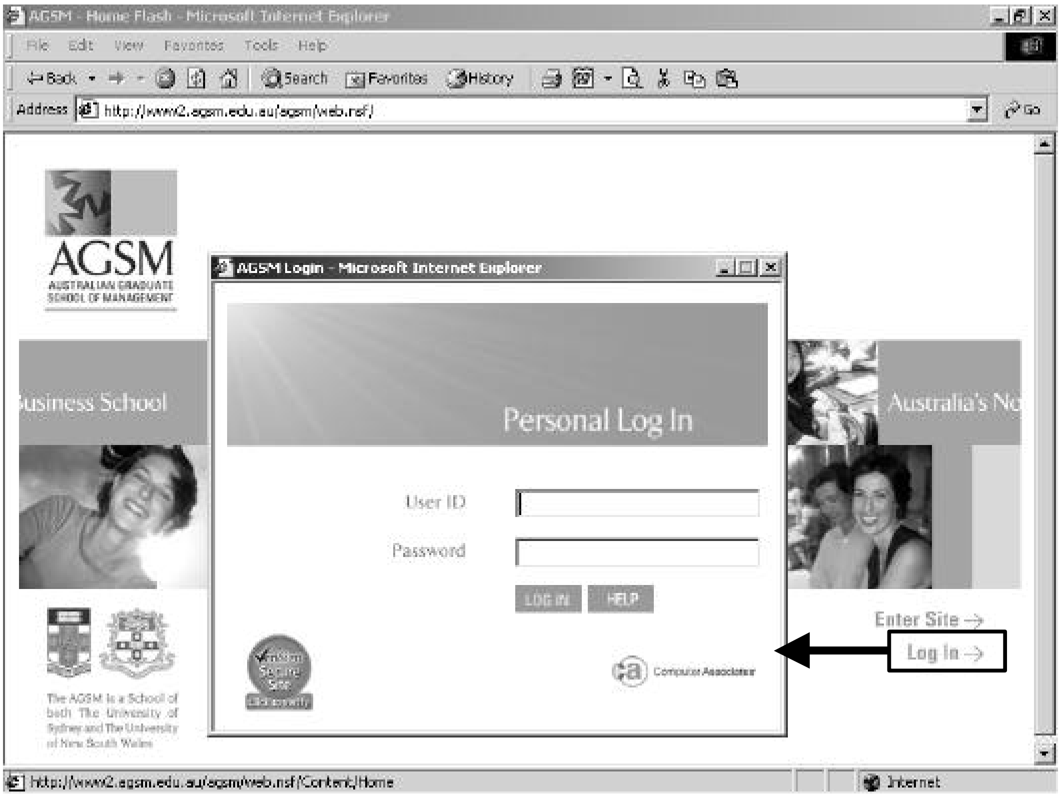
SSO is the backbone of the AGSM's user authentication and authorisation process. When users log on, the SSO determines what policies apply to that particular user ID. After that, the SSO vouches for the user to other systems.

Login Process

SSO employs a three-step process to facilitate user login. Initially, SSO enforces an authentication process, to identify and verify a user at the time of initial login. It then provides the authenticated user with a familiar desktop, containing links or shortcuts to approved applications. Finally, when the user selects an application by simply "pointing and clicking", SSO invokes the application and communicates user credentials to it. This process is transparent to the user, seamlessly allowing access to diverse applications and systems throughout AGSM.

A clear login button is provided on AGSM's web site for the user community to begin the authentication process. Once activated, the user is presented with a GUI login dialog box to begin the process, standardizing the login interface for the user. Regardless of where users login, the "look and feel" of the process is the same.

AGSM web site with SSO login:


AGSM - Home Flash - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www2.agsm.edu.au/agsm/web.nsf/
Go
AGSM
AUSTRALIAN GRADUATE SCHOOL OF MANAGEMENT
Business School
The AGSM is a School of both The University of Sydney and The University of New South Wales
AGSM Login - Microsoft Internet Explorer
Personal Log In
User ID
Password
LOG IN
HELP
Computer Associates
Australia's No
Enter Site →
Log In →
http://www2.agsm.edu.au/agsm/web.nsf/Content/Home
Internet

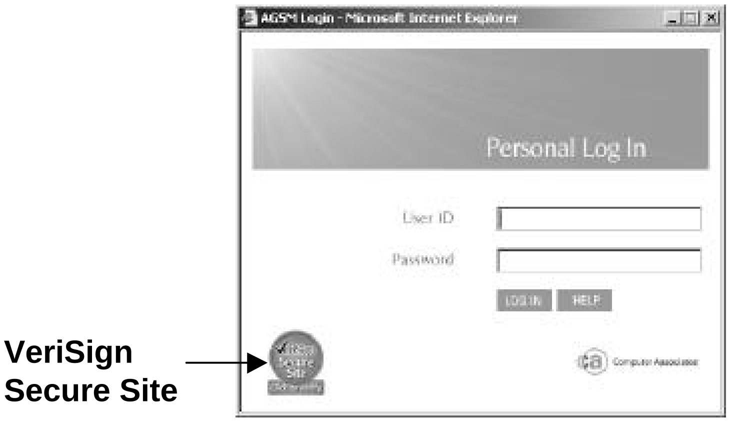
1. The user enters a valid user ID and password for authentication to the SSO Server. This information is encrypted.
2. SSO server verifies the user’s identity and replies to the client with the appropriate application list.
3. The user launches any application through the “My Menu” page on his or her desktop.

SSL Certification

SSO involves granting a lot of access rights, therefore it is important that the single authentication process is secure. On most LANs and WANs, user IDs and passwords are transmitted in clear text and along the network unencrypted. Security can easily be compromised when programs are freely available to capture and reveal these user IDs and passwords or barcode numbers.

Encryption, the process of transforming information to make it unintelligible to all but the intended recipient, forms the basis of data integrity and privacy necessary for e-commerce (Desmarais 2000). AGSM users submit sensitive information and purchase goods and services via the Web. This only happens when they are confident that their personal information is secure.

In order to provide this encryption and protection of information against disclosure to third parties, AGSM recently upgraded the SSO product to use digital certificates whose authenticity is checked against a Verisign Certificate Authority [5].



VeriSign
Secure Site

An SSL Certificate is an electronic file that uniquely identifies individuals and Web sites and enables encrypted communication (VeriSign 2000). SSL Certificates serve as a kind of digital passport or credential. Installing the VeriSign SSL Certificates not only makes online transactions safer for users, it actually makes it easier to submit sensitive information over the Internet.

Internet browsers have built-in security mechanisms to prevent users from unwittingly submitting their personal information over insecure channels. If a user tries to submit information to an unsecured site (a site without an SSL Certificate), the browser will, by default, show a warning, which will lead the user to question the trustworthiness of the site.

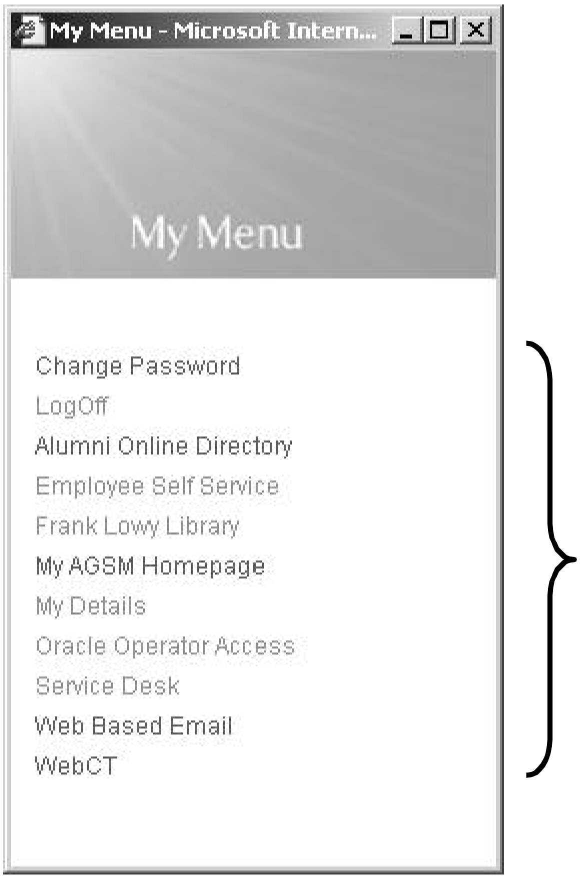
In contrast, if a user submits credit card or other information to a site with a valid SSL Certificate and an SSL connection, the warning does not appear. The secure connection is seamless, making the online transactions more pleasant for the user.

“My Menu” (Launch pad)

SSO automates user login to Web-based applications and platforms by providing a friendly desktop or “launch pad” that is part of a simple “point and click” process.

Each user views a unique page containing personalized content that the system or web administrator wants the user to see. Likewise, if there is information that one or more users should not see, it is easy to prevent them from accessing it.

A typical example of a staff “My Menu” will look like this:



User’s authorized Web applications and resources

"My Menu" is a dynamically built desktop interface, which contains the user's authorized applications, forwarded by the SSO server. It automates application access for users and includes the following additional functionality:

- Time-out or "screen locking" to allow users to securely walk away from their workstations.
- The ability to login as a new user.
- Communication with the SSO server to receive login dialog information and to edit user details as required.

Integrating SSO with ILMS

It does not make sense for libraries, which are part of a larger organisation, to provide their own unique solution to the access management problem. As the SSO database provides the user authentication at the organisation level, integrating it with the ILMS was the single most important achievement for the Library.

At AGSM, the user community comprises mostly students, faculty, staff and alumni. In this ever-changing group, students may leave school in the middle of the term, adjunct faculty may not teach some terms, and staff members may be hired or leave their jobs at any point during the year.

Therefore, the critical question, "*who has access to what*?", is addressed and managed by the administrators of the SSO database. This security administration is the first step in providing the AGSM community with secure and easy access to the "Electronic Library".

The Electronic Library

An electronic library isn't just a Web page. Neither is it just a revamped online public access catalogue (OPAC). An electronic library is the medium by which libraries of all types and sizes provide the knowledge and resources they are used to seeing inside the library's walls – plus much more that is available via the Internet (Byrne 2003).

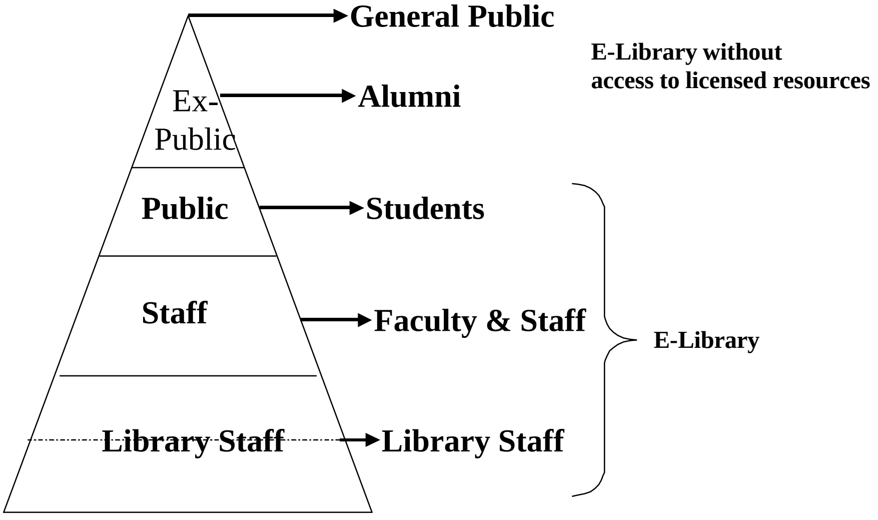
The FLL's Electronic Library provides for its users a gateway to a whole world of organised information and services to support the school's teaching, learning and research needs that are delivered directly to users. These include the Library Catalogue (OPAC), subscription databases, electronic books and journals, digital collections, local publications and resources such as AGSM working papers and much more.

ILMS Access Management

Sirsi's Unicorn[6] ILMS itself provides an integrated solution to the access management problem. In Unicorn, when a library user is added to the system, they are assigned to one or more user groups (e.g. staff, faculty, student, alumni, etc.). The groups are then given access rights to resources. For example, the group "faculty" may be given access rights to more or different resources from those available to the group "student".

The diagram below illustrates this hierarchical scheme for user levels and the associated Electronic Library privileges.

Unicorn User Level



The Integration Process

This “user matrix” is interfaced with the SSO database. As a user's access level or status changes, this change is automatically updated in the library database. For example, as soon as a student user changes status to an alumnus a new file is generated for the library database. When users access the Electronic Library, including remotely, they login once, regardless of the number or type of resources that are available to them. The interaction between the user and the Electronic Library is encrypted using SSO’s secure authentication and ILMS internal login session.

All ILMS-provided solutions are usually designed to interface with the library database. They are not designed to interact with the school’s student database. To overcome this limitation, Unicorn provides batch programs and utilities to upload the user file generated from SSO database into the Library’s user database. Although batch processing does not provide for real time updates to the database, the addition of SSO authentication provides additional flexibility and functionality that outweigh this drawback.

Remote Access Management

The Library employs IP filtering, wherever possible, to control on campus access to its subscription databases and electronic journals. Online content providers need to preserve the integrity of their usage licenses and to protect their resources from unauthorized access while simultaneously providing access to legitimate users. Libraries can also run the risk of jeopardising site licenses if secure access management systems are not in place.

In order to provide remote access to these resources, IP filtering is combined with EZproxy[7], a proxy server technology for libraries developed by Useful Utilities. EZproxy is an easy to maintain program that provides the AGSM user community with remote access to web-based licensed databases. It operates as an intermediary server between the users and the Library's licensed databases. It works by dynamically altering the URLs within the web pages provided by database vendors. Since EZproxy runs on the AGSM network, the database vendor sees the request as coming from a valid IP address, so permits access. The result is a seamless access environment for users. Another added feature of using a proxy server like EZproxy is its powerful statistics and log functions. It allows the Library to gather in-depth statistics on the usage of these resources and help justify budget requests for database licensing.

The integration of SSO with the ILMS provides the Library with an easy authentication solution to control use of the EZproxy server.

Summary and Conclusion

By implementing SSO, not only did AGSM benefit from having a solid authentication and access management system that provided privacy, granularity, and ease of use and maintenance, but it also enabled the Library to make its online resources available to its users from anywhere in the world.

Integrating the SSO product with ILMS has definitely provided a solution for user authentication. It has also allowed the Library staff to be involved more in helping users access online resources than managing the tightening of security to these networked resources.

Also, the access management solutions that are based on "one-for-all" solutions, allow for no granularity in terms of service provision. Thus, the customization of an ILMS's own authorisation and access management to suit the user needs of a library provides high levels of granularity in terms of matching people and resources (See appendix A).

Finally, selecting the right SSO solution depends upon its features. Before even considering integrating it with ILMS, SSO must be able to provide:

- Open Standards compliant technology
- Wide system platform support
- Support for advanced authentication methods.
- Integrated Web SSO support

This open and flexible SSO solution has allowed AGSM to grow as its IT technology and requirements continue to evolve.

Bibliography

Botzum, Keys. (August 2001), *Single Sign On*, [Online], IBM, Available from: <http://www7b.boulder.ibm.com/wsdd/library/techarticles/0108_botzum/botzum.html> [21 August 2003].

Byrne, Alex. 2003, 'Digital libraries: barriers or gateways to scholarly information?', *The Electronic Library*, [Online], vol. 21, no. 5, pp. 414-421. Available from: Emerald [26 August 2003].

Carden, Philip. 1999, 'The new face of single sign-on', *Network Computing*, [Online], vol. 10, iss. 6, pp. 32-42. Available from: Factiva [01 July 2003].

Computer Associates International, Inc. (2000), *White Paper eTrust Single Sign-On: Managing User Access In An eBusiness Environment*, [Online], Available from: <http://www3.ca.com/Solutions/Product.asp?ID=166> [18 June 2003].

Desmarais, Norman. 2000, 'Body language, security and e-commerce', *Library Hi Tech*, [Online], vol. 18, no. 1, pp. 61-74. Available from: Emerald [01 July 2003].

Dix, John. 2001, 'Single sign-on doesn't have to be difficult', *Network World*, [Online], vol. 18, iss. 26, pp. 52-55. Available from: Proquest/ABI-Inform [03 July 2003].

Findlay, Andrew. (March 2000), *Regaining Single Sign-On*, [Online], Available from: <http://www.brunel.ac.uk/depts/cc/papers/regaining-sso.html> [16 July 2003].

Flint, Andrew. 1998, 'Once is enough: single sign-on is simpler, easier', *Computing*, [Online], vol. 24, iss. 28, pp. 30-31. Available from: Proquest/ABI-Inform [23 July 2003].

Fuchs, Ira H. (1998), *Remote Authentication and Authorization for JSTOR*, [Online], Available from: <http://www.jstor.org/about/remote.html> [16 July 2003].

Hazari, Sunil. 2002, 'Challenges of implementing public key infrastructure in Netcentric enterprises', *Logistics Information Management*, [Online], vol. 15, no. 5/6, pp. 385-392. Available from: Emerald [01 July 2003].

Helenius, Tatiana. (1998), 'Online access with a single sign-on', *Wall Street & Technology*, [Online], vol. 16, iss. 10, pp. 70. Available from: Proquest/ABI-Inform [23 July 2003].

Karve, Anita. (1998), 'Authentication Central', *Network Computing Asia*, [Online], August issue. Available from: Factiva [05 July 2003].

Lynch, Clifford. (3 July 2002), *A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources*, [Online], Coalition for Networked Information, Available from: <http://www.cni.org/projects/authentication/authentication-wp.html> [01 July 2003].

Lynch, Clifford. 1997, 'The changing role in a networked information environment.', *Library Hi Tech*, [Online], vol. 15, no. 1, pp. 30-38. Available from: Emerald [29 July 2003].

Services Strategies Inc. (2002), *Secured Single Login Validation*, [Online], Available from: <http://network-protection.com/eTrust_Single_sign-on.htm> [03 July 2003].

VeriSign. (2002), *Guide to Securing your Web Site for Business*, [Online], Available from: <http://www.verisign.com/resources/gd/secureBusiness/secureBusiness.html> [05 August 2003].

Endnotes

[1] *Financial Times* (UK, 2003) rankings.

[2] Asia Inc. (2003) rankings.

[3] See AACSB web site at: <http://www.aacsb.edu>

[4] See Computer Associates web site at: <http://ca.com>

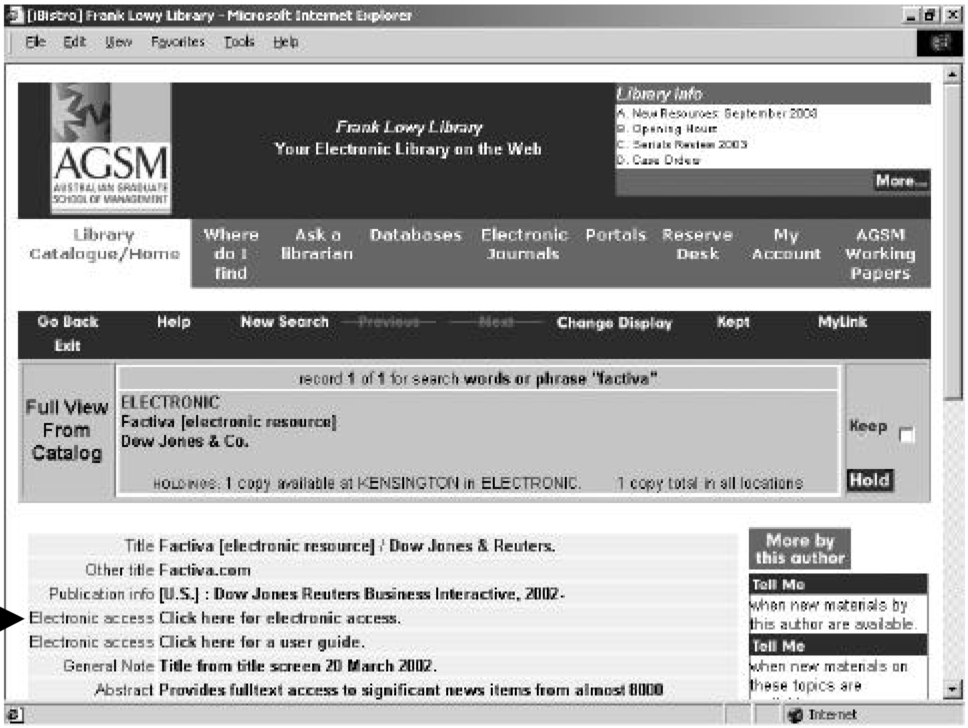
[5] See VeriSign web site at: <http://www.verisign.com>

[6] See SIRSI web site at: <http://www.sirsi.com>

[7] See EZproxy by Useful Utilities web site at: <http://www.usefulutilities.com>

Appendix A

Example of a “Student” login view of OPAC:



record 1 of 1 for search words or phrase "factiva"

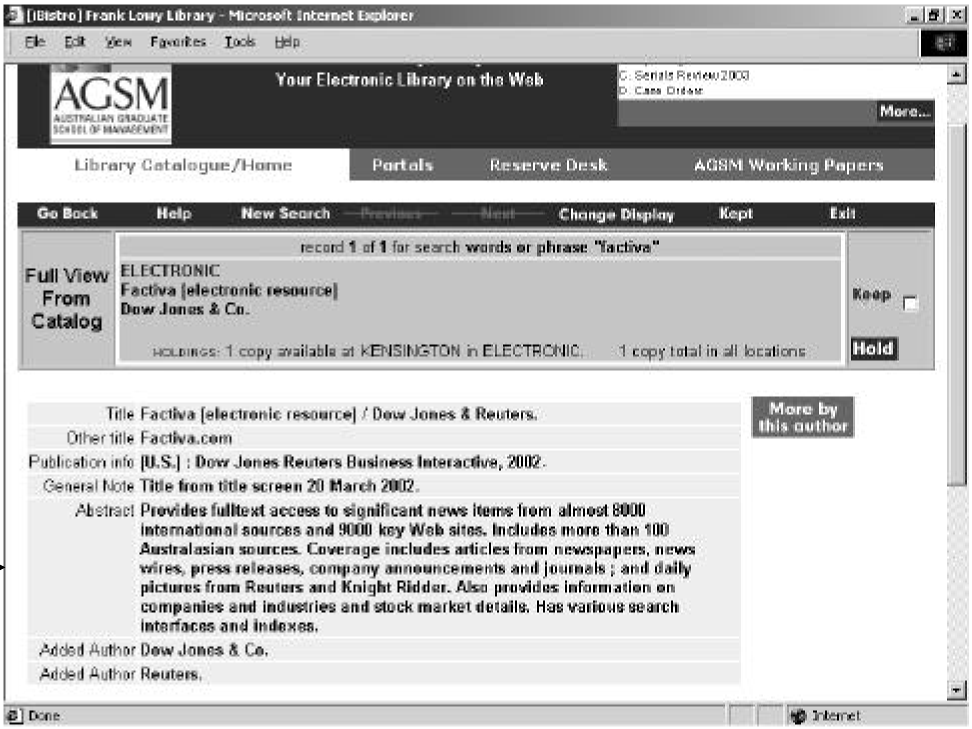
ELECTRONIC
Factiva [electronic resource]
Dow Jones & Co.

HOLDINGS: 1 copy available at KENSINGTON in ELECTRONIC. 1 copy total in all locations

Title Factiva [electronic resource] / Dow Jones & Reuters.
Other title Factiva.com
Publication info [U.S.] : Dow Jones Reuters Business Interactive, 2002-
Electronic access Click here for electronic access.
Electronic access Click here for a user guide.
General Note Title from title screen 20 March 2002.
Abstract Provides fulltext access to significant news items from almost 8000

E-Access

Example of a “General Public” login:



record 1 of 1 for search words or phrase "factiva"

ELECTRONIC
Factiva [electronic resource]
Dow Jones & Co.

HOLDINGS: 1 copy available at KENSINGTON in ELECTRONIC. 1 copy total in all locations

Title Factiva [electronic resource] / Dow Jones & Reuters.
Other title Factiva.com
Publication info [U.S.] : Dow Jones Reuters Business Interactive, 2002-
General Note Title from title screen 20 March 2002.
Abstract Provides fulltext access to significant news items from almost 8000 international sources and 9000 key Web sites. Includes more than 100 Australasian sources. Coverage includes articles from newspapers, news wires, press releases, company announcements and journals ; and daily pictures from Reuters and Knight Ridder. Also provides information on companies and industries and stock market details. Has various search interfaces and indexes.
Added Author Dow Jones & Co.
Added Author Reuters.

No
E-Access