



NLE Technology Report

Authentication and Role-Based-Networking In Libraries



The Power of the Library Card to Enable Library Services in the 21st Century

*NLE Solutions for
Creating and Managing Networks in Libraries*

January, 2009 update





This document is written for librarians and library systems administrators to provide understanding of the purposes of network authentication, and the appropriate technologies to enable role-based network policies and services.

Almost all public libraries today provide computer access to the internet and internal servers located in the library, and almost all “Integrated Library Systems” (ILS) provide or support authentication methods to control and manage the level of computer access. The questions remain:

- Why is authentication technology important for libraries?
- How should libraries apply authentication in the digital library services era?

WHY AUTHENTICATION IS IMPORTANT FOR LIBRARIES

The use of the library card as a method of authentication for other library services beyond “book check-out”, typically leverages the ILS database, and re-purposes protocols such as SIP2. Any library that has deployed a *PC Reservation* software product is probably familiar with this authentication process, and the idea of uniquely identifying the person using the library computers has high value to the library.

The new demands on libraries to manage desktop computers and create new levels of access to information, have led libraries to leverage the library card as the key to access. Since most Information Library Systems (ILS) databases are already populated with patron information that can be used for a standard two form-factor authentication (user-name and password), it is important that these databases can be used appropriately to create a user-friendly experience, while still accounting for who accesses the library purchased media, both printed and electronic.

Libraries do not desire to “re-invent the wheel” by creating new databases, or lists of patrons who are authorized to use the various resources in the library. Controlling access to on-line journals and periodicals through a proxy IP address is becoming obsolete due to the virtual-library concept. Funding for libraries is sometimes based on “use” statistics, it is also important for a library to have data for access to new digital media as well as traditional book check-out.

Authentication in libraries is important for the same reasons that it is important in any computer network environment. When access needs to be verified, controlled, directed, reported, redirected, or denied, authentication is the first mechanism. The intent of



authentication is not to create a burden for the patron, but to verify that the patron is authorized to access information by their status, where they live, by their age of responsibility, etc. We refer to this classification as a “Network Role”. Since libraries classify information each and every day, they can easily relate to the need to classify the types of users that access the library network – *guests, juveniles, city government employees, library staff, conference attendees, city patrons, federated patrons from colleges and universities* – these are all different types of users that should be considered for different “Network Roles”.

Many of the desktop computer management systems that are in use in libraries today utilize some form of authentication to identify the patron, to start the clock to limit the time used at the computer, to verify that the user is authorized to access information based on good standing (no late fines) at the library, etc.

Now, as patrons and guests bring their own personal digital device into the library network, the initial reason for authentication may have shifted, but the consequences of not being able to identify someone who is using the library network is the same. There is a shared community risk when providing open network access without any accountability. There are common-sense observations that people will behave more appropriately to the community standards and good citizenship when they are requested to provide their credentials, regardless of any further restrictions or risk management.

Additionally, in the shifting virtual-library world, access to on-line journal subscriptions still need some level of control, either through proxy IP address access-control-list (ACL), or through individual credential logon. Colorado State University explains why authentication is important to libraries in the most plain and simple terms:

*“The databases provided by CSU Libraries are on the Web but are **not** free. We purchase these from companies. Our agreements with them limit access to CSU employees and registered students. If you are not on CSU's campus, the database companies do not know that you are affiliated with the university, so you are denied access.”*

HOW SHOULD LIBRARIES APPLY AUTHENTICATION TECHNOLOGY?

- ***Public wireless networks need methods of authentication to help protect library network resources, patron-owned computing devices, and the general community:***

The goal for creating a wireless network in libraries is not to create an unsecured open public internet “hot-spot” that invites hackers, spammers, and malicious computer users. The goal is to create a “safe haven” different from the cyber-attack environments that many hot-spots can become. The library should always be a secure sanctuary that allows patrons to use their own networking devices to access library services in a secure and community friendly way.

Patron devices should be kept safe from worms, viruses, and any form of mal-ware. Authentication by itself will not guarantee this. Using “network roles”, which are derived from authentication results, the library can assign users to be scanned by other “unified threat



management” network security devices that will add this layer of protection. Devices and users who are trustworthy can be rewarded for their good cyber-citizenship, and the malicious users can be quickly identified and restricted. Isn’t this how we would expect other community social contracts to be applied and enforced?

Public wireless networks in libraries need to be designed to prevent security risks such as “peer-to-peer” file-stealing, malicious software, “spam” attacks and launching, rogue access-points, denial-of-service attacks, etc. The starting point for this is to utilize authentication.

- ***Public wireless networks in libraries must be able to leverage existing authentication databases without having to re-create the credentials.***

Even a small city public library can have thousands of patrons. The existing database of patron information needs to be utilized, not re-created. The possibility of providing secure on-line governmental services via a web-browser can also be realized quickly by city government if they could enable authentication via the library card credentials – most citizens already have a library card, and otherwise wanting to obtain access to government services may be a good reason to obtain a library card.

- ***Public wireless networks must require no additional client software other than current standard web browsers, etc.***

This is a network design issue for libraries. They need to choose a solution that will allow for authentication via a standard web browser.

- ***Public wireless network will need to be capable of managing multiple levels of security based on type of user (staff, patron, etc.)***

Access control components need to support different policies for different types of users on the wireless network. The library staff will naturally need to have greater access to library servers and information systems, whereas the patron will probably only need access to card-catalogs, electronic media libraries, the Internet, etc. Firewall technology should be used to prevent or allow access and/or visibility. If patrons cannot “see” a server on the network, they will not attempt to attack or create mischief - temptation is removed.

Policies that are “role-based” are the ideal method of delivery. Access control components should also be able to support “role-based” administrative users to enable other library staff to monitor wireless network use, troubleshoot a patron problem, etc.

- ***Public wireless network must have a mechanism to enforce acceptable use policies, Internet content filtering, proxy server redirection, etc.***

Public libraries that use U.S. federal government funds may have the additional requirement to enforce and/or remove Internet content filtering. This may require additional proxy server controls. The wireless network access control components may need the ability to force TCP (port 80) traffic to be redirected to a proxy server.



If the library needs to enforce other “acceptable use” policies, there needs to be methods for restricting a selected user if there is violation of an acceptable use standard. This means that individual user control must be a feature of the access control components.

NLE SOLUTION: AUTHENTICATION AND THREAT MANAGEMENT FOR LIBRARIES

Since 2001, NLE has been providing wireless network and security solutions and services to libraries. NLE solutions help libraries meet the technology challenges of providing for open access to information using patron-owned devices, while maintaining a secure computing environment for the library and the community at large.

Also, NLE was a strategic deployment partner with SirsiDynix for wireless network technology, and implemented their wireless network solutions throughout their product offering period. NLE solutions can work with any library system.

The NLE solution for libraries is the “**Library Application Delivery Suite**”. This is a mix of products and services that elevate the library to the highest standard of protection, ease of use for the staff and patrons, and delivers high value of security to the community. Libraries that are meeting the challenges of transitioning to the digital era are using the “**Library Application Delivery Suite**” from NLE.

CONTACT

NLE ♦ 1276 S. 1380 W. ♦ Orem UT 84058 ♦ 801-377-0074 ♦ www.nle.com ♦ sales@nle.com