Find information about using NCIP authentication to provide access to FirstSearch.

General information

NCIP authentication overview

Library patrons sometimes request access to library services from remote locations. Libraries need to be able to authenticate and authorize access to their services for these remotely located patrons. Proxy servers and similar mechanisms allow libraries to perform these functions, but not without intensive resource commitments (time spent on setup and maintenance, money invested in equipment, etc.). Circulation system patron authentication for the FirstSearch service, through the use of the NISO Circulation Interchange Protocol (NCIP), allows library patrons to gain appropriate access to the FirstSearch service from any location. NCIP is an approved NISO standard that defines messaging between circulation systems, ILL systems, or broker applications. NCIP has many applications, only one of which is authenticating patrons for access to an online service.

The FirstSearch service currently allows manual logon, IP address recognition, scripted access, IP referer, and Athens authentication, none of which provides a complete access solution for all remote users. The NCIP-based patron authentication feature, while it does not replace these existing authentication methods, complements and supplement them.

Local library systems store circulation and patron authentication information that FirstSearch can use for remote patron authentication. To be authenticated for FirstSearch access, a patron must enter information required by the library, which, through its authorization(s), controls who has access to FirstSearch. The end goal is to allow patrons to get into the appropriate FirstSearch account according to their library affiliation(s).

Trust relationships

OCLC and libraries use the NISO Circulation Interchange Protocol to exchange information needed to authenticate a patron for access to the FirstSearch service. Information is requested from a patron and passed securely over https to a library's local system (this means that the local system must support https protocol). The local system then responds and, where possible, sends back more information about the patron. The information passed depends on the purpose of the transaction. Limited information is required to authenticate a patron for individual access to FirstSearch.

Libraries use the NCIP Authentication screen in their FirstSearch administrative module to control the local systems that are configured for NCIP. A library most likely sets up NCIP for its own local system, but it might also set up NCIP for local systems that are geographically close or in its own group. The library retains control of where its patrons' data is exchanged; therefore, OCLC assumes a trust relationship with any local system that is configured for NCIP.

A trust relationship between OCLC and any local system configured for NCIP means that both parties, while not
necessarily agreeing on how to handle patron data, are satisfied with how the other is behaving with respect to that patron data. OCLC acts as a broker in this exchange, so the parties involved are:

- The home library of the patron in question
- The local system with which the patron is interacting at any given time

While OCLC cannot control what a local system does with patron data once it is received, OCLC assumes that the library that configured access to that local system is aware of the system's policies and is satisfied with how patron data is handled and safeguarded. OCLC also safeguards user data, and does not retain this data any longer than it takes to complete the requested transaction.