Newsletter

ALA TechSource
alatechsource.org

Smart Libraries™

Formerly Library Systems Newsletter™

50 East Huron Street, Chicago, Illinois 60611-2795, USA

ISSN 1541-8820 January 2015 Volume XXXV Number 1

Smarter Libraries through Technology: Protecting the Privacy of Library Patrons

By Marshall Breeding

Libraries hold the confidentiality of patron information as a fundamental value. Library automation systems are generally configured not to retain records that reveal the specific materials that a patron has borrowed, at least beyond the operational need. In the consumer arena, to the contrary, details regarding behavior have become a major currency of the economy.

One of the realities of the Internet lies in the ability for any third party to intercept the transmissions of information as it travels among devices and servers. Wireless networks are an especially easy target. Assume today that any information transmitted as clear text across a local network or the Internet will be intercepted and used, whether for targeted advertising or illegal intrusion into servers and systems.

Encryption provides the main line of defense against the unwanted capture of data. The absolute and most basic transaction that demands encryption is the sequence used to authenticate staff and users into a system. Any exposure of username and passwords without strong encryption is an invitation for unwanted access into that system. A further line of defense lies in encrypting sensitive data files, including data stores that hold the personal details such as search and reading behavior or financial transactions.

This issue of *Smart Libraries Newsletter* presents a brief study of the privacy and security characteristics of a sampling of the major automation and discovery products. While results offer a glimpse of the current state of privacy and security in our industry, I present them primarily to increase awareness and to open a broad-based conversation to effect needed improvements.

Conclusions: From Awareness to Action

The results of the survey follow inside, and here I'll present my observations. For many of the providers and products, the level of privacy and security is left to the discretion of their library customers. I would encourage opting for the highest level of security offered. All of the products targeted in this study indicated that they follow standard practices related to the security of passwords and sign-on sequences.

I commend Biblionix for its early move to delivering all transactions for its Apollo ILS via pages encrypted via HTTPS. BiblioCommons states that it will be following that approach beginning in 2015. Full encryption has seen increasing adoption on major destinations with both Google and Facebook moving to that level of security in 2013.

I believe that libraries should work toward comprehensive encryption as the minimal level of security performance expected from these products. No longer is it enough to secure only the transmission of sensitive details, but systems need to protect the general stream of transactions, such as patron searches, selections made, and materials read or downloaded.

Encryption addresses only one layer of the overall environment that relates to privacy and security. Even when patron and staff sessions are fully encrypted, they may expose patron details and reading behavior via cookies or other tokens that may be enabled. When libraries blend services from external social and e-commerce networks into their own environment, there is the strong possibility of the transmission of data elements to those external networks.

I'm not necessarily advocating that libraries follow a flat and sterile approach in their service delivery. As libraries enable these social features, they should be aware of what might be exposed and then carefully manage the process. Some libraries might choose to allow patrons to opt-in after warning them that some details may be provided to the partner site. While individual patrons have their own preferences on privacy, libraries have an additional set of concerns related to the profession's ethics regarding how systems that they provide manage privacy and security.

Privacy and Security of Automation and Discovery Products

This study is an introductory effort to probe at the general characteristics of some of the major integrated library systems, library services platform, and discovery services related to their security and how well they defend patron privacy. A questionnaire of questions on this topic was developed and sent to Auto-Graphics, Biblionix, BiblioCommons, Ex Libris, Innovative Interfaces, OCLC, SirsiDynix, and to the development communities for Koha and Evergreen. These organizations were selected to represent a mix of systems that find wide use in the United States, with the following characteristics:

- **Auto-Graphics** develops and supports the VERSO ILS used primarily by public libraries.
- **BiblioCommons** offers a variety of patron-facing products through a large-scale web-based platform that interoperates with most of the major ILS products.
- **Biblionix** offers Apollo, a purely web-based ILS for small public libraries delivered through a multi-tenant platform.
- **Innovative** now supports an expanded slate of library management products including Millennium, Sierra, Polaris, and Virtua, as well as discovery services such as Encore and Chamo.
- **SirsiDynix** products include Symphony and Horizon as its major ILS offerings, as well as the web-based BLUEcloud suite.
- **OCLC** has developed its WorldShare Management Services and the WorldCat Discovery Service as global multi-tenant platforms used by libraries of all types.
- **Ex Libris**, oriented primarily to academic and research libraries, has developed Alma and Primo as its current set of strategic products for resource management and discovery.
- **Koha** is an open source ILS developed by a global community of developers and used by thousands of libraries of all types around the world.
- **Evergreen**, used primarily by consortia of mostly public libraries in the United States and Canada, is an open source ILS with Equinox Software serving as the dominant development and support firm, supplemented by a global community of developers.

These organizations are to be commended for their prompt response to the questionnaire.

Online Catalog or Discovery Patron Interactions

The initial set of questions focused on how the various products handled transactions conducted by library patrons. Key areas of concern include how well the authentication credentials of patrons are protected and whether all or parts of the session that the patron conducts on the system is protected from detection by a third party as it passes through local networks and the Internet.

Encryption of General Patron Activity

The gold standard for products used by patrons would be to encrypt all traffic conducted by patrons. This level of security would provide private communications for the patron, with very little possibility for leakage and meaningful detection of content by any third party. In the absence of the encryption of the full patron session, third parties can fairly easily intercept data that reveals the search terms entered by a patron, referral data that shows previous sites visited, results presented, and items selected or downloaded for viewing. Full enforcement of encryption requires that the library or its vendor obtain valid digital certificates, perform needed server configurations, and provide the additional processing resources required. Traditionally, library systems have used encryption selectively. Some providers may not enforce encryption by default, but may enable libraries to select encryption for specific transaction types as an option. The questions in this section walk through these possibilities.

1. Enforce encryption through SSL for **all transactions involving patron activity**:

- **Auto-Graphics:** Yes
- **BiblioCommons:** BiblioCommons enforces SSL encryption for all patron activity that is within BiblioCommons environments and involves personally identifiable information. SSL encryption will be extended to all web pages involving patron activity in 2015.
- **Biblionix:** Our online catalog enforces SSL encryption for all patron activity. (*Response extends to all questions in the section.*)
- **Innovative:** Regarding Polaris, Virtua, and Sierra, including their respective OPACs, and Encore and Chamo discovery, the answers are essentially identical. Public searching and discovery all systems support and default to plaintext (HTTP) for searching, and automatically enforce SSL (HTTPS) for all pages involving patron details or login credentials. (*Response carries through all questions in this section.*)
- **SirsiDynix:** All SirsiDynix Software as a Service (SaaS) systems are now deployed with SSL/TLS for HTTPS traffic encryption, and the option is available for existing SaaS customers and for customers which host SirsiDynix products locally to implement the same with SirsiDynix support.
- **OCLC:** Yes. All pages or transactions which contain patron identity data are encrypted for transmission. In the near future, all WorldShare Discovery transactions will be encrypted with HTTPS.
- **Ex Libris:** (*Response applies to all questions in this section.*) All of the patron requesting process is done in Alma mashups embed-

ded in the Primo interface. Like all Alma screens, these are triggered by HTTPS calls only.

Primo uses APIs that communicate with Alma for populating My Account in Primo based on Alma stored information. These APIs respond only to configured and trusted IPs. Primo support for HTTPs for the entire transactions will be implemented next year.

In addition, patron authentication transactions in Primo are encrypted via SSL.

- **Koha:** Out of the box, Koha does not enforce use of SSL. However, every Koha installation can readily be required to use SSL for public catalog and staff interface access.
- **Evergreen:** The Evergreen public catalog requires the use of SSL when logging into the catalog and when accessing all pages that display patron account information or allow the patron to place requests.

2. Offer the library an option to enable SSL for all transactions involving patron activity

- **Auto-Graphics:** Yes
- **BiblioCommons:** No
- **SirsiDynix:** The use of transmission encryption described above is optional for customers, though SirsiDynix informs customers of the risk of unencrypted transmissions and the company's position that no highly sensitive personally identifiable information (i.e., Social Security Numbers, financial account numbers, etc.) be processed or stored with its products.
- **OCLC:** SSL is set by default. No need for institution level management.
- **Koha:** At present, standard configurations of Koha would either require SSL for the entire public catalog or none of it; likewise for the staff interface. (*Response covers multiple questions in this section.*)
- **Evergreen:** The standard configuration of Evergreen mandates the use of SSL for all pages in the public catalog that display patron account information.

3. Enforce encryption for specific pages or transactions involving patron details or login credentials

- **Auto-Graphics:** Yes. If the customer selects the option to enforce encryption, all pages are encrypted, all credentials and all transactions, using SSL. Login and other credentials of the user are encrypted for all systems with or without SSL enabled.
- **BiblioCommons:** Yes
- **SirsiDynix:** If the library enables encryption, as described in above answers, pages processing sensitive information such as patron details and credentials are encrypted.
- **OCLC:** Yes. All pages and transactions that contain patron identity data are encrypted for transmission.
- **Evergreen:** The standard configuration of Evergreen mandates the use of SSL for all pages in the public catalog that display patron account information.

4. Offer the library an option to enable SSL for specific pages or transactions involving patron details or login details

- **Auto-Graphics:** Yes. As noted, if the library enables SSL it is enabled on all pages, all transactions and on all credentials passing in the UI. Login and other credentials of the user are encrypted for all systems with or without SSL enabled.
- **BiblioCommons:** No
- **SirsiDynix:** In line with responses to questions 1-3, typical SSL/TLS deployment encompasses the entire product, which is the recommendation in the security industry.
- **OCLC:** SSL is set by default. There is no need for institution level management.
- **Evergreen:** The standard configuration of Evergreen mandates the use of SSL for all pages in the public catalog that display patron account information

Security of Transactions Conducted by Library Personnel

Another set of questions focuses on the security of the tasks conducted by library personnel on these systems. The accounts used by these individuals may have access to sensitive data related to patron details as well as financial or other institutional data. In addition to whether such data is transmitted securely, it is also of interest to understand whether files are encrypted to prevent viewing by intruders that might gain access. Systems following the highest level of security would encrypt all traffic for staff-related transactions. Few business systems encrypt the storage of all categories of data, but we probe at selected types of data with more sensitive library data, including authentication credentials, patron details, search logs, and financial information. Depending on the system, staff functionality may be provided through software installed on local computers or accessed through web-based interfaces. The mechanisms for security may vary depending on the architecture of these staff clients.

Does your client or interface for delivering functionality to library personnel:

1. Enforce encryption through SSL or other encryption mechanisms for all transactions.

- **Auto-Graphics:** Yes
- **BiblioCommons:** No
- **Biblionix:** The staff interface enforces SSL encryption for all transactions. (*Applies to all questions in this section.*)
- **Innovative:** Regarding Virtua, Polaris, and Sierra, all systems handle communication uniformly for all pages in the staff-facing systems rather than toggling between plaintext and encrypted communications by function or by page. Two systems support SSL for staff client communications; one uses a proprietary non-plaintext communication, not SSL. *(Applies to other questions in this section.)*
- **SirsiDynix:** Virtual Private Network (VPN) is available and recommended for encryption of staff traffic for SirsiDynix

products, both for SaaS- and client-hosted implementations. (*Applies to multiple questions in this section.*)

- **OCLC:** OCLC uses a hybrid model; transactions that provide access to accounts or transactions attributable to an individual patron are encrypted.
- **Ex Libris:** Alma is SSL only. All browser pages are activated only via HTTPS calls. *(Applies to all questions in this section.)*
- **Koha:** The Koha staff interface can be configured to require SSL for all pages, although this is not the default configuration. Most Koha vendors do this as default. (*Covers multiple questions in this section.*)
- **Evergreen:** The Evergreen staff client uses SSL to encrypt all communications with the Evergreen application server. (*Applies to all questions in this section.*)

2. Offer the library an option to enable SSL or other encryption mechanisms for all transactions.

- **Auto-Graphics:** Yes
- **BiblioCommons:** No
- **OCLC:** OCLC configurations are global and SSL/TLS is the default for all patron data.

3. Enforce encryption for specific pages or transactions involving patron details.

- **Auto-Graphics:** Yes. If the customer selects the option to enforce encryption we encrypt all pages, all credentials and all transactions using SSL. Login and other credentials of the user are encrypted for all systems with or without SSL enabled.
- **BiblioCommons:** Yes
- **OCLC:** Yes

4. Enforce Encryption for specific pages involving authentication of library personnel accounts.

- **Auto-Graphics:** Yes. As noted, if the library enables SSL it is enabled on all pages, all transactions and on all credentials passing in the UI. Login and other credentials of the user are encrypted for all systems with or without SSL enabled.
- **BiblioCommons:** Yes
- **OCLC:** Yes

5. Offer the library an option to enable SSL for specific pages involving patron details.

- **Auto-Graphics:** Yes. As noted, if the library enables SSL it is enabled on all pages, all transactions and on all credentials passing in the UI. Login and other credentials of the user are encrypted for all systems with or without SSL enabled.
- **BiblioCommons:** No
- **Biblionix:** Our staff interface enforces SSL encryption for all transactions
- **OCLC:** OCLC configurations are global and SSL/TLS is the default for all patron data. If patron data is presented, it is encrypted.

6. Enforce encryption for specific pages involving authentication of library personnel accounts.

- **Auto-Graphics:** Yes. As noted, if the library enables SSL it is enabled on all pages, all transactions and on all credentials passing in the UI.
- **BiblioCommons:** Yes
- **Biblionix:** The staff interface enforces SSL encryption for all transactions.

7. Offer the library an option to enable SSL for specific pages involving patron details.

- **Auto-Graphics:** Yes. As noted, if the library enables SSL, it is enabled on all pages, all transactions, and on all credentials passing in the UI. Login and other credentials of the user are encrypted for all systems, with or without SSL enabled.
- **BiblioCommons:** No

8. Offer the library an option to enable SSL or other encryption mechanisms for specific pages involving authentication of library personnel.

- **Auto-Graphics:** Yes. As noted, if the library enables SSL, it is enabled on all pages, all transactions, and on all credentials passing in the UI. Login and other credentials of the user are encrypted for all systems with or without SSL enabled.
- **BiblioCommons:** No
- **OCLC:** OCLC configurations are global and SSL/TLS is the default for all patron data. If patron data is presented, it is encrypted.

9. Enforce encryption for transactions involving institutional financial data (acquisitions, patron fines, etc.).

- **Auto-Graphics:** Yes
- **BiblioCommons:** Yes
- **OCLC:** Yes. Account data is encrypted via SSL transactions.

10. Offer the library an option to enable SSL or other encryption mechanisms for financial transactions.

- **Auto-Graphics:** The proper answer is no, as all financial transactions must be secured using SSL, even if no other part of the system is.
- **BiblioCommons:** No
- **SirsiDynix:** SirsiDynix products are designed such that any processing of financial transactions is performed via secure handoff to a PCI DSS-compliant third party; the third party then processes the payment and returns a transaction completion code to the SirsiDynix product as confirmation.
- **OCLC:** OCLC configurations are global and SSL/TLS is the default for all patron and financial data.

Internal Storage of Sensitive Data Elements

How does your platform or system deal with the security of the storage of specific types of data?

1. Does your system store patron passwords or PINs as unencrypted text?

- **Auto-Graphics:** No
- **BiblioCommons:** No
- **Biblionix:** No
- **Innovative:** No
- **SirsiDynix:** SirsiDynix products implement one-way, salted hashing of PINs upon PIN creation, after which the hash is used throughout system functions.

- **OCLC:** No. Identity Information in OCLC's Identity Management System is encrypted using AES-256 encryption.
- **Koha:** No
- **Evergreen:** No

2. Does your system store patron passwords or PINs as salted hash or similar mechanisms?

- **Auto-Graphics:** Yes
- **BiblioCommons:** Yes
- **Biblionix:** Libraries can choose what authentication method they wish to use. Many libraries choose to use a phone number on the patron's account as the patron "password". Other times, they choose straight-up password authentication. Regardless of what the library chooses, any patron may set a password for their own account, which overrides the default authentication and which is stored as a salted bcrypt hash.
- **SirsiDynix:** SirsiDynix products implement one-way, salted hashing of PINs upon PIN creation, after which the hash is used throughout system functions.
- **OCLC:** No. Identity Information in OCLC's Identity Management System is encrypted using AES-256 encryption.
- **Koha:** Koha stores patron passwords using a salted hash (bcrypt).
- **Evergreen:** Evergreen currently stores patron passwords using unsalted hashes.

3. Does your system encrypt patron details as they are recorded and stored?

- **Auto-Graphics:** Yes
- **BiblioCommons:** Yes
- **Biblionix:** Patron details are not encrypted when stored internally.
- **SirsiDynix:** Yes, as described above
- **OCLC:** Yes. For transmission over the open Internet and on disk.
- **Ex Libris:** Personal patron data, such as patron IDs, emails, addresses and phone number are all encrypted in Alma's and Primo databases. The encryption is 2 way using a fixed key.
- **Koha:** Patron information is not encrypted within the MySQL database.
- **Evergreen:** Evergreen does not encrypt patron details in the database.

4. Are logs or other system files that include patron search or reading behaviors encrypted?

- **Auto-Graphics:** Search histories and reading behavior do not contain specific user information. User must opt-in to save their search history as part of their user record, this data is not encrypted. Reading history is also a user specific opt-in option and is not encrypted.
- **BiblioCommons:** Log files are not encrypted, searches are logged at the session level and sessions are not permanently stored.
- **Biblionix:** No, but catalog searches are not stored attached to patrons, and libraries can choose how much patron reading history they want to keep. We plan in the future to allow patrons to override the librarian's settings to keep less history.
- **Innovative:** Regarding Polaris, Virtua and Sierra including their respective OPACs, and Encore and Chamo discovery, none currently encrypt patron details or logs at rest, and all systems but one store PINs as salted hash or similar mechanisms. All systems' technology stacks are capable of encryption at various levels (e.g. at the database table, file, filesystem or storage subsystem level), so differences in current data at rest representation between systems are not constrained architecturally, and enablement of encryption at the filesystem or storage subsystem level would change the at rest stance of all data (logs, PINs, patron details) simultaneously for the system in question.
- **SirsiDynix:** SirsiDynix makes available to SaaS customers the feature of encrypting full sections of the system, protecting the data at rest; log and critical system files are included when this encryption is implemented.
- **OCLC:** Searches that result in holds or requests that are attributable to an individual patron are encrypted. OCLC's Librarian Interface encrypts all transactions including financial transactions and patron identity data.
- **Ex Libris:** Logs are not encrypted, however due to privacy reasons, we don't have any personal information within the logs
- **Koha:** Such logs are not encrypted.

Other Security Measures

Describe any other security measures in place that protect patron privacy as it is transmitted over local networks or the Internet from interception by any third party. One specific scenario that has been a topic of concern involves the presentation of e-book discovery and lending transactions via library catalogs or discovery interfaces.

- **Auto-Graphics:** Overdrive, Recorded Books and similar services are integrated with vendors using SSL. VERSO does encrypt (using SFTP) files being submitted to collection agencies.
- **BiblioCommons:** Communication to ILS systems are over SSL.
- **Biblionix:** We make no distinction between local networks and the Internet, so our HTTPS-only policy protects against attackers and MitM everywhere.

  We have never and will never allow any patron data to be sent unencrypted over the wire. NCIP is all over HTTPS. SIP is done via SSH tunnels or via SSL, and we require client-side certificates for both. We've encountered resistance on this from some ebook vendors, but the libraries always back us up when the issue is explained to them.

  We've helped many of them configure their systems to work with us, and we've developed a tunnel installer that makes it easy for librarians to use PC management software (and similar) from within the library.

  In some cases, third-party services expect library patrons to visit their sites and log in with their card number and password, which they then validate via SIP with Apollo (over a secure connection, of course).

If the library directs the patrons to go through Apollo to access these services, as we recommend, then we can submit the login information to the third-party service. When we do so, we use a randomly-generated, temporary password. This way, the patron's real password is never submitted to the third party.

- **Innovative:** Regarding Polaris, Virtua and Sierra, APIs handling patron data support SSL (HTTPS) and are password and/or key protected.
- **SirsiDynix:** In addition to the protection offered through the use of data transmission encryption as described in the first section above, SirsiDynix recognizes the need for security to be "baked in" from the foundation of a web application upward. As a great volume of security breaches occur due to improperly or ineffectively programmed software—opening up the web applications to a host of established and ever-evolving attack types—SirsiDynix has adopted Open Web Application Security Project (OWASP) security standards for its development. This includes incorporation of security efficacy checks throughout the Software Development Life Cycle (SDLC), including peer and objective code reviews; Security Vulnerability Assessments (SVAs)—both automated and manual—performed by developers throughout the development cycle and again by testers as part of the release gate analysis; specific testing of each release against the most common system environment permutations (i.e., operating system, web server, and database software); and testing against the latest security patches for environment software. In this way, the latest releases will address the current security issues from a software perspective, providing customers with confidence that the privacy of staff and end user information is protected. This level of security integration is also in line with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53/Federal Risk and Authorization Management Program (FedRAMP) and International Organization for Standardization (ISO) 27001 security standards to which SirsiDynix has been or will be certified by external audit, as described at the end of this questionnaire.
- **OCLC:** All patron data is encrypted via SSL/TLS 2048. Open discovery searches are non-attributable to an individual patron. Searches that result in holds or requests that are attributable to an individual patron are encrypted. Librarian interfaces are encrypted for all transactions. OCLC understands that the confidentiality, integrity and availability of our members' information are vital to their business operations and their success. OCLC uses a multi-layered approach to protect key information by constantly monitoring and improving applications, systems, and processes to meet the growing demands and challenges of dynamic security threats. In recognition of security efforts, OCLC has met ISO 27001 security standards and has received registrations. OCLC has adopted the OWASP security standards for application security and has integrated security and privacy in our Product Management Life Cycle.
- **Ex Libris:** Primo and Alma's data in transit communication is being encrypted. Whether this is a browser communication via SSL or secured FTP. The encryption is made using industry standard encryptions such as SHA. As related to the specific scenario, all of the patron requesting transactions are done in Alma mashups embedded in the Primo interface. Like all Alma screens, these are triggered by https calls only.
- **Koha:** Koha can be configured to use an LDAP directory to authenticate staff users and patrons. If configured this way, LDAP-over-SSL can be used to encrypt communications between the Koha and LDAP servers.
- **Evergreen:** Evergreen can be configured to use an LDAP directory to authenticate staff users and patrons. If configured this way, LDAP-over-SSL can be used to encrypt communications between the Evergreen and LDAP servers.

Vulnerabilities Introduced via Third Party Integration

Describe any integration with third party organizations that could potential expose patron details, search, or reading patterns and measures that you have provided to strengthen privacy and security.

- **Auto-Graphics:** None
- **BiblioCommons:** Many third-party integrations have been implemented on the BiblioCommons service at the request of partner libraries, who have contracted both fees and privacy and security standards directly with the suppliers. These include OverDrive, 3M Cloud Library, Axis 360, Content Cafe, Syndetics, and Zola Books.

  BiblioCommons has also entered into contracts directly with integration partners, which has allowed BiblioCommons to implement privacy security standards by agreement. Examples include LibraryThing, Zola Books, Google Analytics, FoxyCart (e-commerce payment gateway) and iDream Books.

  BiblioCommons recently cancelled a commercial Share-This service, used for posting content from the catalog to various social media channels, because our agreement did not provide prevent patron IP addresses from being shared with ad networks. The service has been replaced with a new native sharing service that interacts with 3rd-party sites only upon a patron's request.
- **Biblionix:** Patron details: A hole in SIP is that there isn't a way in the specification to pick and choose which data is shared with the third party. We're working with the NISO SIP working group to address this in the next version. In the meantime, we're

working on (but have not yet released) a way for the library to select which SIP client is allowed to see what information about patrons.

Search: Search history is not exposed in any way.

Reading patterns: It's possible for an (authenticated and encrypted) SIP client to look up patrons and see their list of items currently out. If this is done frequently enough, it could become a way for third parties to compile a checkout history. As stated above, Biblionix is looking into options to allow libraries to share only what is needed with SIP clients.

- **Innovative:** Regarding Polaris, Virtua and Sierra, for the purpose of such integrations, encrypted, password protected methods may be used as described above.
- **SirsiDynix:** SirsiDynix now includes provisions in all contracts with such third parties (i.e., those providing integrated service enhancements, payment processors, etc.) legally requiring these parties to comply with, at a minimum, the NIST SP 800-53 Low baseline security standard, as this baseline is sufficient for private sector and most government operations. See the SirsiDynix Controlled Access Plan (CAP) item AC-SD-a. for policies and procedures related to these activities. Additionally, as seen in the SirsiDynix Privacy Policy (http://www.sirsidynix.com/privacy), the company commits to protection of user privacy—including search and reading patterns—and never discloses or facilitates disclosure of individual user Personally Identifiable Information (PII) or behavior. The actions SirsiDynix has taken to ensure user privacy have been verified via audit performed by TRUSTe and the company has been issued the TRUSTed Cloud certificate of privacy protection.
- **OCLC:** OCLC does not share patron information with third parties unless explicitly authorized in the contract or in written authorization with the library. OCLC conducts third-party service provider risk assessments and ensures that any contracts with TSPs include the appropriate controls to protect data from unauthorized disclosure. In the United States, OCLC has mapped its controls to NIST 800-53 to demonstrate compliance with the U.S. Federal Information Security Management Act. Additionally, OCLC ensures security and privacy controls meet the requirements of various international bodies such as the European Network and Security Agency and German Federal Office for Security of Information Technology (BSI).
- **Koha:** SIP2

Vulnerabilities Through APIs

1. Do the APIs allow or require encryption in requests or responses that include patron-related data?

- **BiblioCommons:** Our APIs support SSL.
- **Biblionix:** We don't have custom APIs, only some XML feeds (which contain no patron data), SIP (encryption requirements discussed above), and NCIP (which is over HTTPS and so is exclusively encrypted).
- **SirsiDynix:** Encryption support is provided via the mechanisms described in the first section of the questionnaire.
- **OCLC:** Yes. OCLC encrypts all connections sharing privacy data via an encrypted connection specific to the library.
- Ex Libris The APIs security is based on protocol security. There is no encryption of payloads.
- **Koha:** Various Koha web services can be set up to require use of SSL.

2. What limitations to security impact your system, imposed by the APIs or protocols managed by external or third-part products?

- **Auto-Graphics:** Auto-Graphics, uses protocols such as SIP2, Z39.30 and NCIP (1 & 2), some of these protocols do not use encryption, but they are typically not used to pass patron specific data, as outlined above. NCIP is offered both with and without SSL depending on the other vendor's implementation.
- **BiblioCommons:** Some 3rd party APIs are provided via a mixture of HTTPS and HTTP. We use HTTPS when available and consideration is given to any API using HTTP.
- **Biblionix:** No external or third party products. SIP limitations discussed above.
- **Innovative:** Regarding Polaris, Virtua and Sierra, APIs handling patron data support SSL (HTTPS) and are password and/or key protected.
- **OCLC:** Third party business partners and vendor risk assessment is completed and controls are implemented based on the risk or as specified at higher levels by the provider. OCLC does not share patron information with third parties unless explicitly authorized in the contract or in written authorization with the library. APIs are managed through the API specifications.
- **Ex Libris:** The APIs security is based on protocol security. There is no encryption of payloads.
- **Koha:** A variety of service providers communicate with Koha systems using SIP2. SIP2 is inherently an insecure protocol, and with very few exceptions, typically is not operated in a secure fashion. However, these services can be secured with the addition of a VPN or SSH tunnel to the service endpoints.
- **Evergreen:** Information about library purchases can be transmitted to materials vendors via EDIFACT EDI; not all vendors, however, require the use of an encrypted protocol such as SFTP or FTPS.

  A variety of service providers communicate with Evergreen systems using SIP2. SIP2 is inherently an insecure protocol, and with very few exceptions, typically is not operated over an encrypted transport such as a VPN or an SSH tunnel.

ALA TechSource
alatechsource.org

Smart Libraries Newsletter
American Library Association
50 East Huron Street
Chicago, IL 60611-2795 USA
Address Service Requested

January 2015
Smarter Libraries through Technology

Smart Libraries Newsletter

Marshall Breeding's expert coverage of the library automation industry.

Editor
Marshall Breeding
marshall.breeding@librarytechnology.org
Twitter: @mbreeding

Managing Editor
Patrick Hogan
312-280-3240
phogan@ala.org

TO SUBSCRIBE

To reserve your subscription, contact the Customer Service Center at **800-545-2433, press 5 for assistance**, or visit **alatechsource.org**.

The 2015 subscription price is $85 in the United States and $95 internationally.

ALA Techsource purchases fund advocacy, awareness, and accreditation programs for library professionals worldwide.

Digital Access for Subscribers
alatechsource.metapress.com

Production and design by the American Library Association Production Technology Unit.

Smart Libraries Newsletter is published monthly by ALA TechSource, a publishing imprint of the American Library Association.

alatechsource.org