ISSN: 3070-4030

Mini Review

World Journal of Tourism Management

Application of Cryptology to Libraries: Tourism Resources are Safer

Gregory K. Tharp*

Independent Researcher, U.S

***Corresponding Author**
Gregory K. Tharp, Independent Researcher, U.S.

Submitted: 2026, May 28; **Accepted:** 2026, Jun 30; **Published:** 2026, Jul 07

Citation: Tharp, G. K. (2026). Application of Cryptology to Libraries: Tourism Resources are Safer. *World J Tourism Mgm, 2*(2), 01-02.

As global tourism is asked to do more with less in view of declining funding and a changing economic landscape, the application of cryptology to library technical services offers a potential solution to increasing tourism efficiency as they rely on libraries to access tourism information. Through examining the ALA Privacy guidelines found on the ALA website, the need for technical services auditing Integrated Library Systems or ILS is evident in the ALA toolkit on protecting privacy in library systems and is enumerated in the National Information Standards Organizations or NISO Consensus Principles, however the NISO frameworks for secure data exchange between libraries and vendors are one piece of the library privacy puzzle at least from a technical standpoint in that technical services librarians interact with metadata and preservation of library materials and thus need guidance on how to ensure data privacy, ranging from protecting patron information to mundane technical services functions such as copy cataloging, in an era when there are increasing calls from both internal and external parties to cut down library funding in academic, special, public, and other types of libraries due to declining revenue sources, grants, and other reasons [1,2].

For that reason libraries must move away from the NISO's SSO or single sign-on and patron authentication approach cryptographically protecting information without exposing personally identifiable information or PPI to exploring the Library of Congress's PREMIS or Preservation Metadata implementation strategies calling for detailed logging of cryptographic checksums and 'fixty check' events to prove data integrity to support the long-term preservation of digital objects using an international metadata standard and the Digital Preservation Coalition or DPC's data preservation and data integrity standards towards a library cryptology scheme informed by emerging standards to efficiently protect library technical services information. As a little bit of background information about the current DPC cryptography efforts, the DPC Handbook [3,4]. is consulted and reveals standard operating procedures for technical service and archival units regarding 'Bitstream Preservation', outlining the frequency and deployment of SHA-256 and MD5 hashing algorithms to combat data rot, which taken together provides an overview of the current state of library cryptology for technical services and paves the way for a discussion of library information security infrastructure.

The currently proposed library security infrastructure run on two parallel tracks: efforts by the Library Freedom Project or LFP and the ISO/IEC 19790: 2025 standards [5,6]. The LFP is a clinician-led initiative that helps libraries deploy cryptographic tools offering excellent documentation on implementing HTTPS/TLS across Online Public Access Catalogs (OPACs) and deploying privacy-centric routing. While the ISO/IEC 19790:2025 standards help advanced institutional technical services (especially in federal or large research libraries) develop the security requirements for the cryptographic modules used inside data-at-rest encryption databases. Examples of institutional technical policies are aplenty as many university libraries publish their digital preservation policies openly, which serve as excellent case studies for cryptography in action in libraries. Take the Bodleian Libraries at University of Oxford (Bodleian Libraries, 2026) and the National Archives of Australia are examples of preservation policies in that their published Digital Preservation Policies provide real-world frameworks on how cryptographic fixity checking and secure encrypted protocols (like TLS) are mandated during the ingest and maintenance of technical collections [1]. This overview paves the way for a discussion of how cryptology is the backbone of library technical services infrastructure.

Protecting user privacy in circulation and access is important as technical services departments handle vast amounts of Patron Personally Identifiable Information (PII) and circulation histories. Cryptology ensures this data remains confidential through use of data-at-rest encryption, data-in-transit or TLS/SSL, and anonymization and hashing. In data-at-rest encryption, Library Management Systems or LMS and Integrated Library Systems or ILS use symmetric encryption algorithms (like AES-256) to encrypt patron databases. If a server is physically compromised,

the data remains unreadable [1-8]. While in data-in-transit or TLS/SSL encryption, when a patron logs into their account to renew a book or search the OPAC, Transport Layer Security or TLS encrypts the data passing between the user's browser and the library server, preventing eavesdropping. Lastly, in anonymization and hashing, to maintain circulation statistics without violating privacy laws, technical services can use cryptographic hash functions (like SHA-256) which converts a patron's ID into a unique, irreversible string of characters, allowing libraries to track that a book was borrowed without knowing who borrowed it.

Another area where libraries use cryptology is in secure vendor integrations which primarily occurs in e-resources or electronic resources and procurement areas of the library in that modern libraries rarely operate in a vacuum; technical services constantly exchange data with book jobbers, serials vendors, and e-resource providers. API Security and Tokens are used when the LMS automatically orders books via EDI or Electronic Data Interchange and or updates e-book availability from vendors like OverDrive in these exchanges are secured using cryptographic keys and OAuth tokens. In another application, Single Sign-On or SSO and SAML are used to manage access to hundreds of proprietary databases that require secure authentication. Protocols like Shibboleth or Open ATHENS use asymmetric (public-key) cryptography to verify a patron's institutional identity to a third-party vendor without ever revealing the patron's actual credentials [1-8]. Another area where cryptology is used in library technical services is in digital preservation and data integrity in that a core tenet of technical services is ensuring that digital assets, chiefly the institutional repository, digitized archives, remain uncorrupted over decades.

Cryptographic checksums which is when a digital object is ingested into a preservation system, technical services generates a cryptographic checksum (a digital fingerprint using algorithms like MD5 or SHA-256). Also, fixity checking in that periodically, automated systems recalculate the checksum of the stored file. If the new checksum matches the original, the file is intact [1-8]. If it differs, the library knows the file has suffered from "bit rot" or unauthorized tampering, allowing them to restore a backup. Another area in which libraries use cryptology is in digital rights management or DRM and controlled digital lending in which acquisitions and collection management rely heavily on cryptology to comply with copyright laws while maximizing access. For instance, in E-Book DRM, cryptographic wrappers restrict how e-books can be shared, copied, or printed, ensuring publishers' copyright protections are maintained. In controlled digital Lending (CDL): For libraries digitizing physical books to lend them out on a 1-to-1 ratio, cryptographic access controls ensure that the digital file expires and becomes unreadable on the user's device once the loan period ends, preventing illicit duplication. In summation, while cryptology offers a way to safeguard tourism information that tourism relies on, additional studies need to keep pace with emerging information systems threats [1-8].

References

1. American Library Association. (ALA). “Library Privacy Guidelines: Library Privacy Guidelines—Overview and Listing”. (2026). Last modified June 10, 2026.
2. National Information Standards Organization. (NISO). “NISO Consensus Principles on Users’ Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Principles)”. (2015). Last modified June 10, 2026
3. Library of Congress. “PREMIS: Preservation Metadata Maintenance Activity”. (2026). Last modified June 10, 2026.
4. Digital Preservation Coalition. (DPC). “Digital Preservation Consultancy”. (2026). Last modified June 10, 2026.
5. Library Freedom Project. “We are Library Freedom Project”. (2026). Last modified June 10, 2026.
6. ISO. “ISO/IEC 19790: 2025 Information Security, cybersecurity and privacy protection—Security requirements for cryptographic modules”. (2025). Last modified June 10, 2026.
7. National Archives of Australia. (NAA). “Preservation Policy 2021-2025”. (2026). Last modified June 10, 2026.
8. Library Freedom Project. “We are Library Freedom Project”. (2026). Last modified June 10, 2026.