The Lebanon Public Libraries (Lebanon, NH), with the Westchester Public Library System (Westchester County, NY), The Cherry Hill Public Library (Cherry Hill, NJ), and the LEAP Encryption Access Project (LEAP) will develop software called LibraryVPN which will allow libraries to host a Virtual Private Network (VPN) for their patron's use.

VPNs can keep people from harvesting and selling your data, prevent malicious actors from seeing your traffic when connected to open wifi, and help prevent other types of online tracking which compromise people's privacy. There are currently two main barriers to making VPNs more widespread.

1. People don't know which VPN companies to trust - VPNs providers can potentially monitor all of your traffic. If the VPN provider is not trustworthy they could sell your data (like hotspot shield was accused of doing, or even harvest all your browsing data for their own use (like Facebook's VPN app reportedly did).
2. All reputable VPN providers cost money - Although some reputable providers do have a free tier, the data caps are very low. This leaves a situation where the most economically vulnerable are the most likely to be exploited online as well.

LibraryVPN solves both of these issues by hosting the VPN in a trusted institution that is likely already working on privacy issues. Patrons will know that their data will not be abused for profit and all patrons, regardless of their economic circumstances, can have the benefits of a VPN available to them.

This grant will be the first phase of the LibraryVPN project and aims to produce a product that can be trialed by a small number of test libraries. In the second phase, feedback produced by this phase will be incorporated to make the product ready for general adoption by libraries. The third phase of this project would involve promoting it to libraries and assisting libraries with adoption.

LEAP has years of experience building VPN software based on OpenVPN. For the first phase, they will produce three specific deliverables.

1. A Windows Client for LibraryVPN - LEAP already has Mac and Linux clients that can be adapted for use by LibraryVPN. However, a Windows client will provide access to a much larger audience.
2. SIP2 Authentication for LibraryVPN - This will allow library systems to authenticate VPN users using their Integrated Library System (ILS) over the industry standard SIP2 protocol.
3. Setup test instances at a small number of alpha tester libraries to get initial feedback on the software and produce bug reports and documentation to allow for a larger group of beta testers in the next phase of this project.

We expect this phase to take about a year. Eight months for development and four months for testing. At the end of this phase we will have an initial version of LibraryVPN project, and ultimately libraries will be better able to protect their patron's online privacy, even when patrons are not within the library's walls. The result will be strong security and privacy protections available to all of the library's patrons regardless of their financial status. Additionally, this will provide libraries with more outreach opportunities. By showing their value in digital security, they can further engage with their communities.

LibraryVPN

Lebanon Public Libraries requests a **1 year National Leadership grant** in the amount of **$75,200** to **fund the first phase of the LibraryVPN project**. Along with the LEAP Encryption Access Project (LEAP), Cherry Hill Public Library, and the Westchester Library System, the Lebanon Libraries will pilot a **self-hosted Virtual Private Network** (VPN) **service**, “LibraryVPN”, **for use by library patrons**. This project will make it possible for them to safeguard their information online regardless of their financial resources or location.

The Lebanon Public Libraries, Cherry Hill public library and the Westchester Library System all have a history of improving digital security for their patrons by teaching digital security classes and making privacy software available on library computers. As libraries active in the digital privacy space they are ideally suited to help to develop this software. They bring a wealth of knowledge gathered over years of engaging with patron’s on these issues.

LEAP is a US-based non-profit founded in 2012 and dedicated to giving all internet users access to secure communication. LEAP makes it possible for any service provider to easily deploy secure services and for people to use these services without needing to learn new software or change their behavior. These services are based on open, federated standards and always released under free software licenses, which ensure that the software is and will ever remain free. The secure services LEAP helps to provide are designed to respect users’ privacy, and open source protocols are used in the most secure way possible. LibraryVPN will benefit from the knowledge and experience accumulated in years of active development and deployments led by LEAP.

Bringing together the public library experience of our library partners with LEAP’s experience in developing secure, easily deployed software will result in a product that is usable, safe, easy to maintain, and meets the real-world needs of library patrons.

Maturity Level

This project is the **first phase** of a planned three phase project. At the end of this phase, LibraryVPN should be developed to an Alpha testing level. This will be suitable for a small group of 3 to 4 public libraries to try out. These testers understand that there will be bugs and things to need to be fixed in LibraryVPN. They will work to improve documentation and report bugs.

The **second phase** will consist of improving the software based on feedback and experience from the alpha test group. We will then recruit a larger group of beta testers to do a larger scale rollout and ensure that the software is ready for general adoption. We are hoping to have around 12 libraries participate in the beta test program.

The **third phase** will promote general adoption of LibraryVPN by libraries and their patrons. This phase will consist of making the library community aware of the offering and assisting libraries with adoption. LEAP is planning on offering consulting services and support contracts for libraries at this point. This will not only help libraries by having knowledgeable partners to turn to if they have issues or questions, it will provide ongoing funding for continued development of LibraryVPN that is not

contingent on grant funding. There is a possibility that LEAP will also develop a hosted version of LibraryVPN, similar to how Omeka.net offers hosted Omeka instances to help fund development.

Statement of National Need

People are increasingly concerned by attacks on their online security and privacy. Those who cannot afford broadband access in their home have to rely on free public wifi hotspots where security can be minimal and there are no built in security or privacy protection. Even those who can afford their own internet service have reason to worry about applications abusing their access to gather information and sell it for profit.

Libraries already provide internet access to a wide variety of people, especially to economically vulnerable populations and those who are not technologically sophisticated. Patrons who rely on this service benefit from the security and privacy the libraries provide, but only so long as they are physically within the library.

Virtual Private Networks (VPNs) provide a solution to this problem by securely routing all traffic from your device through your VPN provider to the internet. This encrypted tunnel ensures that no one on the local network, or on the network path between you and your VPN provider, can sniff your traffic to see where you are connecting to, how long you are spending there, and even (for non HTTPS connections) all of the information send to and from websites.

However, there are several problems with current VPN offerings.

First, all reliable VPN solutions require a monthly fee. This puts them out of reach of those who are most vulnerable to exploitation. They are already in the position of using publicly available internet connections which puts their security and privacy at risk, and because of their financial circumstances they cannot take advantage of the technology which can protect them.

The second problem is that using a VPN requires people to place their trust in whatever VPN company they use. Some (especially free solutions) have proven not to be worthy of that trust by leaking or even outright selling customer data or containing malware[1]. These companies are taking advantage of vulnerable populations who are unable to afford more expensive solutions or who do not have the knowledge to protect themselves. This creates a situation of only having security and privacy available to those who can afford it and have the knowledge to protect themselves.

Libraries are ideally positioned to help with this situation. Libraries historically have worked to provide privacy and security to people, are located in almost every community in the United States and enjoy a high level of trust from the public. Libraries also care deeply about providing services to all members of their community, regardless of financial circumstances. Some might object to public libraries hosting software that allows people to be anonymous online, but many mainstream sources such as the Freedom of the Press Foundation[2], the Wall Street Journal[3], and the Electronic Frontier Foundation[4] all agree that using a VPN is an important part of maintaining privacy and security on the internet today.

[1] https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf
[2] https://freedom.press/training/choosing-a-vpn/
[3] https://www.wsj.com/articles/why-you-need-a-vpnand-how-to-choose-the-right-one-1537294244
[4] https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

By hosting a VPN service for their patrons, libraries will ensure that all patrons will have access to a trustworthy provider who will not sell their data, and will actively work to protect their privacy and security. The American Library Association's Code of ethics reads, in part, "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted." LibraryVPN will provide libraries with another tool to accomplish this.

Project Design

Grant funding will support the achievement of three major milestones for phase one of the project:

1. Development of modules for the integration of the LibraryVPN platform with Integrated Library Systems (ILS) using the SIP2 protocol

LibraryVPN will support the Standard Interchange Protocol (SIP2) for authentication. SIP2 is supported by many ILS vendors. By building to this standard, we will ensure that libraries hosting VPN services as well as their patrons will be able to rely on existing credentials and authentication mechanisms, making the deployment of the service and the adoption of the VPN client easier. This feature is estimated to take 4 months to complete.

2. Complete a Windows client for library patron use

Currently the vast majority of computer users run Windows as their operating system. LEAP has previously created VPN clients for OSX (Mac), and GNU/Linux that can be adapted to use with LibraryVPN, but the existing Windows Client is still in a beta phase that needs further development to reach stability. Among the development work needed for a production ready client is the development of a windows firewall to avoid privacy leaks, the improvement of a build script that produces an user-friendly installer, and an stable graphical interface. We consider the production of a mature windows client an essential feature to ensure the widest possible applicability of LibraryVPN.

3. Deployment, documentation, training and bug fixing

LibraryVPN will be a free and open source product. This means that any library system that wishes to deploy it on their own should be able to. A key to this is to have bug free software with good documentation. This step will support a test deployment in 2-4 alpha tester library systems. These libraries will test the product and report their findings to LEAP for further development and help to document the product to allow easy deployment by future libraries. The timeline for this stage of the project will depend on how many bugs are found, but is currently estimated at taking 4 months.

Technical Design of Project

Technical Summary

LibraryVPN will be a personal VPN service for increased privacy and security, which encrypts all the traffic entering or leaving the library patrons' devices - including all web traffic. To make this possible, it sends all internet traffic through an encrypted connection to a LibraryVPN server, where it then goes out onto the public internet.

LibraryVPN will be built using LEAP's whitelabel VPN solution, BitmaskVPN[5]. In 2012 LEAP created the Bitmask client[6] to provide encrypted email and VPN access. In 2018, LEAP turned this battled-tested app into an elegant white label VPN solution redesigned to provide a minimal screen footprint and one-click end user experience. The codebase for the VPN application was re-engineered in Go with a focus on customer branding, portability and ease of development. In 2018 LEAP partnered with Riseup[7] to launch their branded version of BitmaskVPN, RiseupVPN[8]. Along with the BitmaskVPN Desktop and Android[9] applications, LEAP has created an automated open source solution for provisioning, deployment, and monitoring of a VPN provider[10] that deploys secure options by default. As a result, the LibraryVPN solution will have state of the art security and ease of use for the end user, and a well documented and trouble-free way of provisioning VPN servers for new libraries that decide to adopt LibraryVPN.

Furthermore, BitmaskVPN is built on OpenVPN[11]. A de-facto industry standard, OpenVPN is a popular and actively maintained open-source VPN solution. By leveraging an existing product that allows for the deployment of an out-of-the-box solution for VPN service provisioning, LibraryVPN service will benefit from ongoing development from the community, and the resulting low-cost maintenance and ability to incorporate enhancements to the service.

The BitmaskVPN product already offers important features that enhance the use of plain OpenVPN. A zero-configuration experience is the most important, but security-wise it is worthy to mention the development of a multi-platform fail-close firewall, and the hardening of the OpenVPN binary by distributing a copy of it that is statically linked against MbedTLS (formerly PolarSSL) - instead of using OpenSSL, which has been plagued by important security vulnerabilities in the past years. Interestingly, part of these BitmaskVPN enhancements were later deployed by a hardened build of OpenVPN[12] commissioned by the Dutch National Security Agency.

Finally, a key development in this project is adding an authentication module to allow libraries to use their existing Integrated Library System to authenticate their patrons. This, along with LibraryVPN's localization features and flexible branding strategy will allow LibraryVPN to integrate seamlessly with libraries that choose to adopt it.

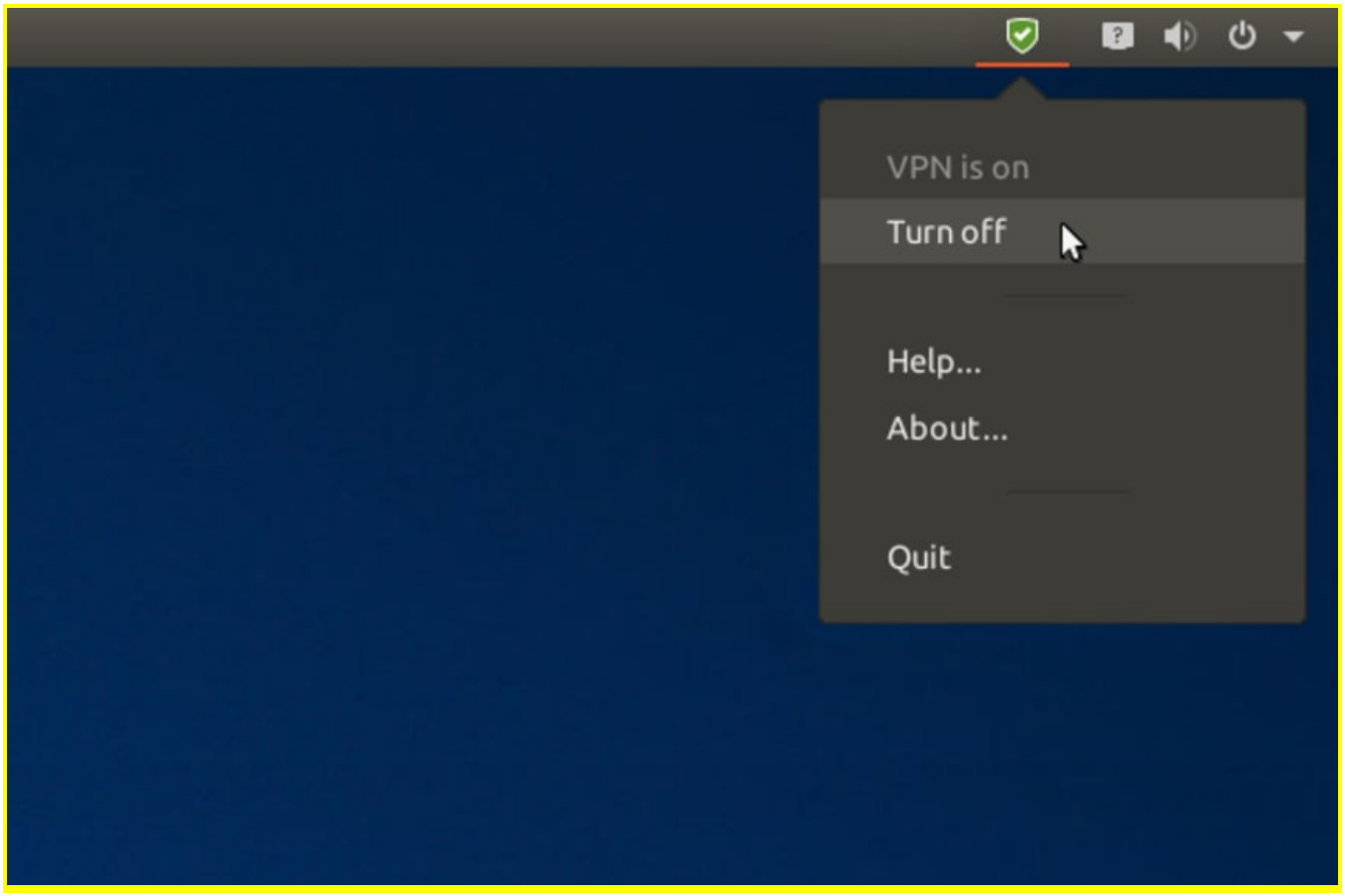
User story: How LibraryVPN works

LibraryVPN will have simple frictionless onboarding. A Patron hears about a new online safety technology that the library is providing for free. The patron goes to the library website which contains easy to parse information, testimonials from other users and clear infographics describing LibraryVPN. The patron downloads the app to their personal computer and launches LibraryVPN. They are now protected by a best in class VPN wherever they go.

The LibraryVPN desktop application has a **minimalistic user interface**: when started, it displays a **shield icon** in the systray. The displayed icon changes according to the status of the connection.

[5] https://0xacab.org/leap/bitmask-vpn
[6] https://bitmask.net/ This codebase and service is in maintenance mode. All recent development is happening on the BitmaskVPN codebase.
[7] https://riseup.net
[8] https://riseup.net/en/vpn/betatest
[9] https://play.google.com/store/apps/details?id=se.leap.bitmaskclient&hl=en_US
[10] https://leap.se/en/platform
[11] https://openvpn.net/community/
[12] https://openvpn.fox-it.com/

Clicking on this icon displays a menu that allows LibraryVPN to be switched on or off, and has options to get help and display an "About" dialog.



In order to connect, user clicks on the "Turn on" menu item. If this is the first time that LibraryVPN is started on this machine, a dialog will pop up, prompting the user to enter her patron card number and optionally a password if the library has their ILS set up to require one. A checkbox will allow users to choose to have LibraryVPN remember their credentials on a given computer. After receiving valid credentials, the application then connects to the LibraryVPN server and the shield icon turns green.

To disconnect, the user simply clicks on the "disconnect" menu item. Upon correctly closing the tunnel, the shield icon becomes gray.

Gray icon: VPN is disconnected.

Yellow icon: VPN is connecting.

Green icon: VPN is connected.

Red icon: VPN connection has failed. Internet is blocked, user intervention is needed.

In the case of any error during initiation or termination of the secure tunnel, a red icon with a hand appears - the status message indicates that the connection is in a failed state, and that the application is blocking the internet. The user can then either retry the connection, or manually cancel the connection attempt and choose to allow unprotected access to internet.

Requirements for integration

There are three basic requirements for the integration of LibraryVPN with the existing Integrated Library Systems. They are further described in the Supporting Document "**Technical Requirements for Integration**".

1. The VPN service must interoperate with the authentication system in place in the Libraries, which is based in a Patron Identifier and, optionally, a passphrase.
2. The user experience with the application must be very intuitive: this is, it should not require any extra effort to the end user. User interface must not be intrusive, and should require a minimal effort to configure a VPN tunnel.
3. Librarians should be able to monitor general metrics about the service.

Design considerations

The authentication system used by most of the Integrated Library Systems is the **Standard Interchange Protocol,** which is a proprietary standard for communication between library computer systems and self-service circulation terminals. Although owned and controlled by 3M, the protocol is published and is widely used by other vendors. Version 2.0 of the protocol, known as SIP2[13], is a de facto standard for library self-service applications.

The authentication components of the LibraryVPN **must interoperate with the existing solutions** for user management provided by the Integrated Library Systems. Libraries use ILS's made by different vendors, and interoperability between the different systems must be ensured. Even though the LibraryVPN system deploys its own authorization measures, the ILS of each library remains the authoritative source of data regarding patron information. However, some caveats must be taken into account when implementing the integration of the authentication system, due to the nature of the SIP protocol and their intrinsic limitations.

Use of encryption

The SIP protocol has no built in encryption, so steps must be taken to send the connection through some sort of encrypted tunnel. In the context of the integration of the LibraryVPN service, two common methods will be used:

- On the server side, **stunnel**[14] will be used to expose the Library's SIP2 endpoint (provided by the ILS vendor) to the LibraryVPN authentication service.
- The communication between the LibraryVPN client and the LibraryVPN authentication service will be protected by Transport Layer Security (**TLS**)[15].

[13] http://multimedia.3m.com/mws/media/355361O/sip2-protocol.pdf
[14] https://www.stunnel.org
[15] https://en.wikipedia.org/wiki/Transport_Layer_Security

These measures ensure that, while in transit, the patron's credentials remain protected against eavesdroppers and malicious agents in the physical medium, both in the communication between the LibraryVPN application and the LibraryVPN authentication service, and between the LibraryVPN authentication server and the Integrated Library System.

Integration targets

The initial target vendor for integration will be **Koha**[16], which is the first free and open source software library automation package, and is the ILS in use in the Lebanon Public Libraries and the Cherry Hill Public Library. Its development is sponsored by libraries of varying types and sizes, volunteers, and support companies from around the world. Koha allows for the configuration of a SIP2 endpoint[17], which will be enabled and configured to be reachable from the LibraryVPN authentication service.

If different ILS vendors are used by the libraries participating in this first phase, efforts will be made to ensure the integration is working in spite of possible deviations of the protocol.

Defense against abuse and possible attacks

As part of the initial design, a detailed risk assessment will be performed, and corrective measures proposed. Although the a priori risk of exploitation of the system is low, since no sensitive information about users is stored, and no new valuable assets are added to the system as a whole, in order to minimize the feasibility and impact of possible attacks (like Denial of Service or user enumeration attacks), very simple countermeasures can be added to the system. These include:

- Rate-limitation on the LibraryVPN authentication endpoint.
- Rate-limitation and sanitization of input to the SIP2 endpoint.
- Use of least privileges, as recommended, on the account configured on the SIP2 endpoint in the ACS server.

Modularity and code reuse

The execution of this project will pay special attention to the principles of modularity and code reuse. This implies several benefits:

1. A mobile client is not included in the roadmap for the current phase, but the need to reuse any used library in a mobile implementation will be highly considered when deciding on the final architecture and the technologies to use. By doing it so, a future android or iOS integration can be executed with minimal cost by reusing components developed in this phase.
2. As stated above, the LibraryVPN product is a customization of an existing codebase. In as much as possible, the specific needs will be integrated into the product in a modular way, so that the future maintainability costs are kept low, and the LibraryVPN application can benefit of updates, bug fixes and code improvements in a seamless way, without affecting the features tailored for the libraries specific use case.

Open Source Code

[16] https://www.koha-community.org/
[17] https://koha-community.org/manual/18.05/en/html/apis_protocols.html#using-sip2

The principles of open source software are very important to all partners in this project. It benefits from the security and continued development of upstream project and will be released under a Free Software License to ensure that it will remain free so that any library can make use of this project. To that end, all the development is made in the open, including tracking of feedback from users, feature requests and continuous code reviews -with the exception made of possible critical security issues-, and all deliverables will be made available in a public code repository under a Free Software License (preferable GPL3 or similar).

Privacy and anonymity concerns

In order to guarantee the user's right to privacy and anonymity, the design of the system includes a decoupling between authentication and authorization and the actual access to the VPN service. As described in the "Implementation details" document, upon a successful authentication using the ILS credentials, the client downloads a certificate from a certificate pool. This certificate is valid for a given period of time to authenticate against the VPN server, but does not contain any personal information pertaining to the user.

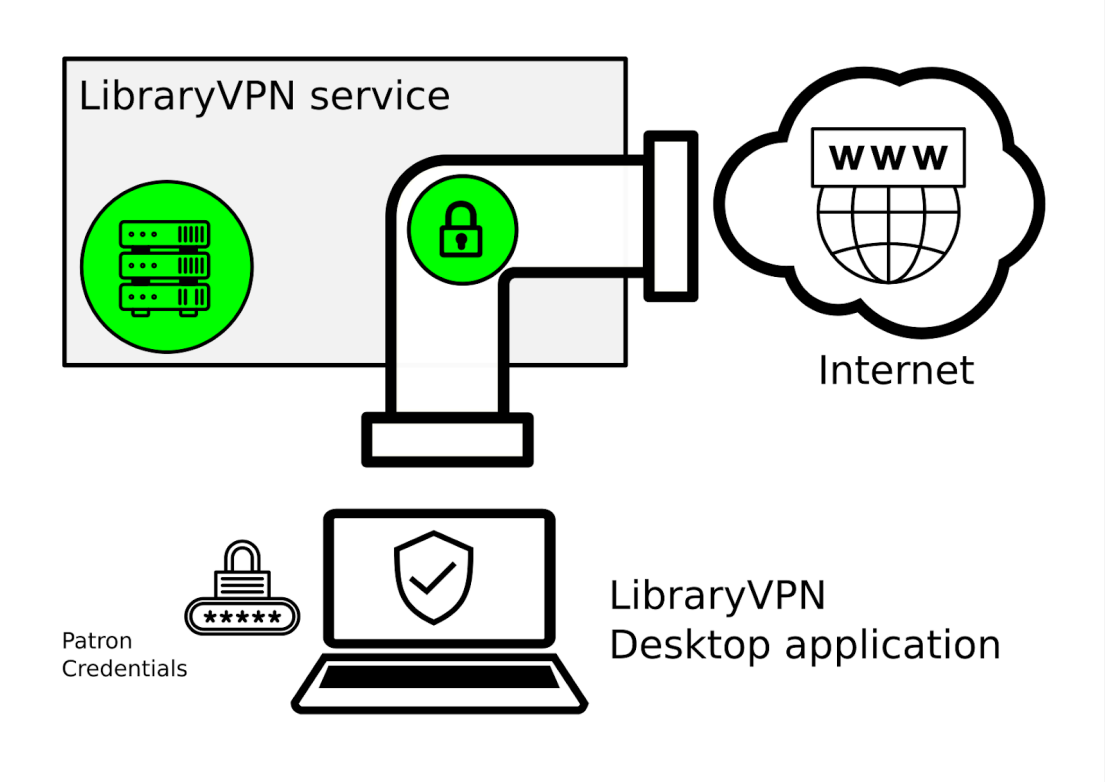
As specified in the "Use of encryption" section, the LibraryVPN traffic will be secured so that patron credentials will not be subject to eavesdropping as it establishes the encrypted tunnel. This will be true even if the tunnel is being established over a shared medium such as wifi.

In addition, the LibraryVPN client will include a firewall that is activated before initiating the encrypted tunnel, which reduces the risk of user profiling by taking advantage of DNS leaks or any other potential attack that relies on unsecured inbound or outbound connections with a destination or origin in the user's device.

On the server side of the LibraryVPN, special precautions will be taken to anonymize any user data when aggregating the metrics that feed the statistics collection module.

Architectural Design

As depicted in the following diagram, LibraryVPN is composed of several services running on the server-side, and a client-side application. Please refer to the supporting document "**Proposed implementation details**" for more information about the preliminary architectural design, implementation details and a brief description of the involved components. The LibraryVPN service will be hosted by the library using LibraryVPN. The LibraryVPN Desktop Application will be installed on the patron's computer.



Performance goals and outcomes

For this grant to be considered successful the following goals will be met:

1. An Alpha testing level of the LibraryVPN software will be complete.
2. The LibraryVPN client software will be able to authenticate against a library's ILS using the SIP2 protocol.
3. The LibraryVPN client software will be available for the Windows operating system.
4. 2-4 library systems will have piloted hosting the software as Alpha testers.
5. Client and server software will be available for download on Github so additional testers can provide feedback in phase two.
6. Preliminary Documentation will be done for additional testers in phase two

Future Plans

After successfully completing phase one of this project, we hope to secure funding from the IMLS or a similar funding organization for phases two and three.

Phase 2 - Beta Testing

Phase two will increase the number of libraries testing the software to ensure that it is ready for widespread use within the library community. Using lessons learned from phase one testing, we will improve the product and then release it to a larger beta test group of libraries. We are currently hoping to recruit around 12 library systems to act as beta testers for phase two. A wider range of libraries testing the software will help to ensure that the software will be ready for general release by the end of phase two.

Phase 3 - General Availability

Phase three of the project will be to support general adoption. Phase three will consist of increasing awareness of the project and providing training and support to libraries that wish to deploy it. We hope to partner with a national organization that has expertise of this type of work such as the Electronic Frontier Foundation or the Mozilla foundation.

National Impact

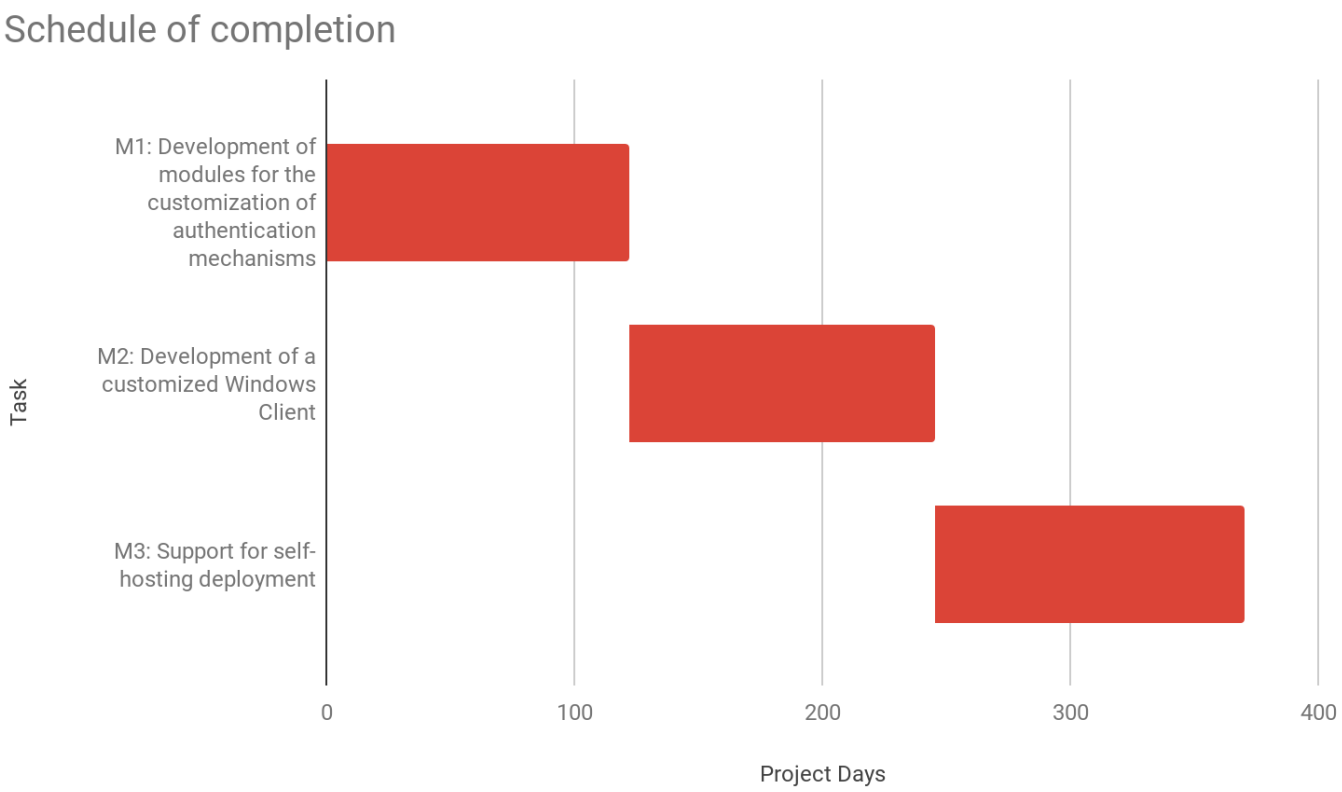
Many libraries already offer patron programming aimed at privacy and security. Libraries are supposed to reduce barriers to accessing information, and fear and uncertainty about privacy and security online certainly represent barriers that prevent people from taking full advantage of the amazing wealth of information that the internet offers us.

Libraries currently host services for patrons to ensure that all members of their community have access to those services regardless of their financial circumstances. They also assist people who do not possess the technology training to access these services through classes and one on one help. Whether these services are online databases, streaming movies, or downloadable ebooks, they represent a large (and growing) portion of a library's offerings.

This project combines these two services to extend library practices into a new, and extremely relevant, area. By hosting a VPN for patron use, they ensure that strong security and privacy protections are made available to all of the library's patrons regardless of their financial status or technical abilities. This will mean less patrons scared to use online resources, less patrons who are exploited by unethical online companies, and fewer people unable to have the protections that those with the financial and technical ability can currently access.

As an added bonus, this will provide libraries with more outreach opportunities. By showing their value in digital security, they can further engage with their communities. Positioning themselves as a place that their patrons can come with security and privacy questions will only help libraries and their communities. Libraries will be able to demonstrate their continued relevance and patrons will have somewhere to go for answers that is not motivated by profit and greed to exploit them. The Lebanon Public Libraries have already experienced this in their own community. Once the library became known as a resource for digital security and an institution that worked to protect people's privacy, many more members of the community started coming to the library to ask questions and get advice. This increase was strictly due to word of mouth with no advertising done by the library. This is an area that people want to know who they can trust. Libraries can fill that role as they always have in the past.

Expected beginning of the project: 15th July 2019



DIGITAL PRODUCT FORM

Introduction

The Institute of Museum and Library Services (IMLS) is committed to expanding public access to federally funded digital products (e.g., digital content, resources, assets, software, and datasets). The products you create with IMLS funding require careful stewardship to protect and enhance their value, and they should be freely and readily available for use and re-use by libraries, archives, museums, and the public. Because technology is dynamic and because we do not want to inhibit innovation, we do not want to prescribe set standards and practices that could become quickly outdated. Instead, we ask that you answer questions that address specific aspects of creating and managing digital products. Like all components of your IMLS application, your answers will be used by IMLS staff and by expert peer reviewers to evaluate your application, and they will be important in determining whether your project will be funded.

Instructions

All applications must include a Digital Product Form.

☐ Please check here if you have reviewed Parts I, II, III, and IV below and you have determined that your proposal does NOT involve the creation of digital products (i.e., digital content, resources, assets, software, or datasets). You must still submit this Digital Product Form with your proposal even if you check this box, because this Digital Product Form is a Required Document.

If you ARE creating digital products, you must provide answers to the questions in Part I. In addition, you must also complete at least one of the subsequent sections. If you intend to create or collect digital content, resources, or assets, complete Part II. If you intend to develop software, complete Part III. If you intend to create a dataset, complete Part IV.

Part I: Intellectual Property Rights and Permissions

A.1 What will be the intellectual property status of the digital products (content, resources, assets, software, or datasets) you intend to create? Who will hold the copyright(s)? How will you explain property rights and permissions to potential users (for example, by assigning a non-restrictive license such as BSD, GNU, MIT, or Creative Commons to the product)? Explain and justify your licensing selections.

Chosen license is GPLv3. This ensures that all the released improved versions be free software, and avoids the risk of having to compete with a proprietary modified version of the software developed during this project.
See https://leap.se/en/source
The property rights will be held by LEAP. As a non-profit devoted to the creation and maintenance of free software and the maintenance of the common codebase, legal consultants advise that a single organization related to the production of the product is in the best position to enforce the GPL in court against violators. In order to achieve this, we need to keep the copyright status of the program as simple as possible. We do this by asking each contributor to either assign the copyright on contributions to the FSF, or disclaim copyright on contributions.

A.2 What ownership rights will your organization assert over the new digital products and what conditions will you impose on access and use? Explain and justify any terms of access and conditions of use and detail how you will notify potential users about relevant terms or conditions.

Conditions for access and use are described in the text of the license mentioned in the precedent point. Said license is displayed in a prominent place and distributed together with the copies of the programs that constitute the deliverables of the work.
In addition, a note about the terms of use that the General Public License Version 3 grants to the user of the software will be prominently displayed in, at least but not limited to:
The only product page
The code repositories
The documentation of the product
The “About” dialog in the desktop application

A. 3 If you will create any products that may involve privacy concerns, require obtaining permissions or rights, or raise any cultural sensitivities, describe the issues and how you plan to address them.

In order to guarantee the users right to privacy and anonymity, the design of the system includes a decoupling between authentication and authorization and the actual access to the VPN service.
On the side of the platform, special precautions will be taken to anonymize any user data when aggregating the metrics that feed the statistics collection module.
For more details, check the “ Privacy and anonymity concerns ” in the Full Narrative document.

Part II: Projects Creating or Collecting Digital Content, Resources, or Assets

A. Creating or Collecting New Digital Content, Resources, or Assets

A.1 Describe the digital content, resources, or assets you will create or collect, the quantities of each type, and the format(s) you will use.

A.2 List the equipment, software, and supplies that you will use to create the content, resources, or assets, or the name of the service provider that will perform the work.

A.3 List all the digital file formats (e.g., XML, TIFF, MPEG) you plan to use, along with the relevant information about the appropriate quality standards (e.g., resolution, sampling rate, or pixel dimensions).

B. Workflow and Asset Maintenance/Preservation

B.1 Describe your quality control plan. How will you monitor and evaluate your workflow and products?

B.2 Describe your plan for preserving and maintaining digital assets during and after the award period of performance. Your plan may address storage systems, shared repositories, technical documentation, migration planning, and commitment of organizational funding for these purposes. Please note: You may charge the federal award before closeout for the costs of publication or sharing of research results if the costs are not incurred during the period of performance of the federal award (see 2 C.F.R. § 200.461).

C. Metadata

C.1 Describe how you will produce any and all technical, descriptive, administrative, or preservation metadata. Specify which standards you will use for the metadata structure (e.g., MARC, Dublin Core, Encoded Archival Description, PBCore, PREMIS) and metadata content (e.g., thesauri).

C.2 Explain your strategy for preserving and maintaining metadata created or collected during and after the award period of performance.

C.3 Explain what metadata sharing and/or other strategies you will use to facilitate widespread discovery and use of the digital content, resources, or assets created during your project (e.g., an API [Application Programming Interface], contributions to a digital platform, or other ways you might enable batch queries and retrieval of metadata).

D. Access and Use

D.1 Describe how you will make the digital content, resources, or assets available to the public. Include details such as the delivery strategy (e.g., openly available online, available to specified audiences) and underlying hardware/software platforms and infrastructure (e.g., specific digital repository software or leased services, accessibility via standard web browsers, requirements for special software tools in order to use the content).

D.2 Provide the name(s) and URL(s) (Uniform Resource Locator) for any examples of previous digital content, resources, or assets your organization has created.

Part III. Projects Developing Software

A. General Information

A.1 Describe the software you intend to create, including a summary of the major functions it will perform and the intended primary audience(s) it will serve.

The LibraryVPN platform is a set of packages that simplify and automate the deployment of a VPN service with hardenization measures and secure defaults. Target audience are system administrators in the Library Community that are willing to deploy the VPN service on their infrastructure.

A.2 List other existing software that wholly or partially performs the same functions, and explain how the software you intend to create is different, and justify why those differences are significant and necessary.

There are many commercial VPN products offered as a service, but none of them provide a solution that is ready to use covering both the provisioning of the service and an easy-to-use application facing the end-user, while remaining as a Free/Open Software product.
OpenVPN, upon which LibraryVPN will be built, is an open source project that allows to setup servers and configure clients, but lacks a multiplatform user-friendly user interface that is able to be setup without the user providing a configuration file.
The system developed by LEAP allows for a one-click setup of the client application, and at the same time offers the added value of a fail-close firewall that blocks any outgoing or incoming traffic - this prevents privacy problems such as DNS leaks.

B. Technical Information

B.1 List the programming languages, platforms, software, or other applications you will use to create your software and explain why you chose them.

The client is written mainly in Go, for portability. The Go toolchain allows for efficient builds and simplifies deployments. The client is currently using the systray library developed by the lantern project: https://github.com/getlantern/systray - for the completion of this project other alternatives will be evaluated, mainly to comply with the widget requirements derived from the need to introduce credentials from within a systray menu. Qt5 will be evaluated for this, as well as solutions based on webkit like https://github.com/zserge/webview

B.2 Describe how the software you intend to create will extend or interoperate with relevant existing software.

Customizations on LibraryVPN will be based on a preexisting product, named BitmaskVPN, which is a generic white label product built on top of OpenVPN that also interacts with the LEAP platform to bootstrap the configuration files. The authentication integration will basically add an authentication mechamism to allow libraries to use Integrated Library Systems to authenticate their patrons.

B.3 Describe any underlying additional software or system dependencies necessary to run the software you intend to create.

For LibraryVPN application, OpenVPN is a dependency, but will be shipped together with the installers or the distribution packages.
For the server, a Debian Linux operating system with ssh access is expected. At least 2 public ips are required for the server.

B.4 Describe the processes you will use for development, documentation, and for maintaining and updating documentation for users of the software.

We use agile development methodology, work in code sprints, use TDD (test driven development) and have a continuous integration workflow along with weekly user testing of new development. This combination of automated testing, running code, and regular hands-on testing by team members as well as a group of volunteer code testers allows for very fast feedback that informs our iterative development process.

We are a distributed team. Our developers and administrators have their own computers, and servers for organization and software development and testing.

B.5 Provide the name(s) and URL(s) for examples of any previous software your organization has created.

Bitmask Client
https://bitmask.net/
http://demo.bitmask.net
https://github.com/leapcode/bitmask-dev
https://bitmask.readthedocs.org

BitmaskVPN
https://github.com/leapcode/bitmask-vpn
https://play.google.com/store/apps/details?id=se.leap.bitmaskclient&hl=en_US

C. Access and Use

C.1 We expect applicants seeking federal funds for software to develop and release these products under open-source licenses to maximize access and promote reuse. What ownership rights will your organization assert over the software you intend to create, and what conditions will you impose on its access and use? Identify and explain the license under which you will release source code for the software you develop (e.g., BSD, GNU, or MIT software licenses). Explain and justify any prohibitive terms or conditions of use or access and detail how you will notify potential users about relevant terms and conditions.

GPLv3

C.2 Describe how you will make the software and source code available to the public and/or its intended users.

DEVELOPMENT
LEAP will make the VPN codebase accessible in a public repository. This codebase includes build script to configure the particular details for a given set of libraries, and the execution of this script in the proper development environment will produce a set of installers to distribute the software for the target operative systems.
LibraryVPN codebase will be freely available, mainly as a set of optional extensions that reuse the original product in as much as possible.
Assistance will be provided to build, properly sign and distribute the software.

USE
Cherry Hill Public Library, and the Westchester Library System, the Lebanon Libraries will pilot a self-hosted Virtual Private Network (VPN) service, “ LibraryVPN ”, for use by library patrons. This project will make it possible for them to safeguard their information online regardless of their financial resources or location. This first phase will be followed by a second phase during which the partners will recruit a larger group of early adopters, and later a third phase of general adoption of LibraryVPN by libraries and their patrons.
Patron will access the VPN via a landing page linked from the main Library Website

C.3 Identify where you will deposit the source code for the software you intend to develop:

Name of publicly accessible source code repository:

https://github.com/leapcode

URL:

https://github.com/leapcode/LibraryVPN // https://github.com/leapcode/libraryvpn_platform

Part IV: Projects Creating Datasets

A.1 Identify the type of data you plan to collect or generate, and the purpose or intended use to which you expect it to be put. Describe the method(s) you will use and the approximate dates or intervals at which you will collect or generate it.

A.2 Does the proposed data collection or research activity require approval by any internal review panel or institutional review board (IRB)? If so, has the proposed research activity been approved? If not, what is your plan for securing approval?

A.3 Will you collect any personally identifiable information (PII), confidential information (e.g., trade secrets), or proprietary information? If so, detail the specific steps you will take to protect such information while you prepare the data files for public release (e.g., data anonymization, data suppression PII, or synthetic data).

A.4 If you will collect additional documentation, such as consent agreements, along with the data, describe plans for preserving the documentation and ensuring that its relationship to the collected data is maintained.

A.5 What methods will you use to collect or generate the data? Provide details about any technical requirements or dependencies that would be necessary for understanding, retrieving, displaying, or processing the dataset(s).

A.6 What documentation (e.g., data documentation, codebooks) will you capture or create along with the dataset(s)? Where will the documentation be stored and in what format(s)? How will you permanently associate and manage the documentation with the dataset(s) it describes?

A.7 What is your plan for archiving, managing, and disseminating data after the completion of the award-funded project?

A.8 Identify where you will deposit the dataset(s):

Name of repository:

URL:

A.9 When and how frequently will you review this data management plan? How will the implementation be monitored?