



Lighthouse Global Case Study

www.lighthouseglobal.com

Industry

Enterprise Software and Services

Business Challenge

Lighthouse was managing its Public SSL and Private certificates manually, requiring significant time to install and renew certificates and putting the organization at risk of expired certificates, costly website outages, and not fully adhering to standards when retrieving client data.

Solution

In 2018, Lighthouse enlisted Sectigo to supply, discover, and manage high volumes of digital certificates across servers, devices, internal applications, clients, and website—from a single pane of glass. With Private PKI, the team was able to deploy certificates throughout their enterprise using auto enrollment capabilities for Active Directory joint computers and workstations.

Sectigo Products

Sectigo Certificate Manager
Sectigo Private PKI
DV, OV and EV SSL Certificates
Code Signing Certificates



Discover certificates issued by any trusted CA on internal and external networks



Visibility into renewal status of every certificate, along with enterprise-wide reporting



Able to issue and install 10,000 certificates within a few weeks

Lighthouse provides eDiscovery, information governance, and compliance services that solve organization's toughest challenges. Since 1995, the Seattle-based company has evolved from moving pallets of paper to managing petabytes of data globally and providing technologies and tailored services to Fortune 500 companies and Am Law 100 law firms. The fastest-growing company in its field, Lighthouse manages the complex landscape of enterprise data for compliance and legal teams, partnering with multinational industry leaders, global law firms, and software providers, to assist with litigation or governmental investigations and minimize the potential for future incidents.

Blindly Fighting System Outages

Lighthouse was managing its SSL and private certificates manually, without auto discovery or enrollment. The enterprise experienced outages that crippled critical systems and put the consulting business at risk, but the IT team was unable to identify where or why the website, applications or other systems were not functioning. The lack of certificate transparency worsened following acquisitions, which were common with a high-growth global organization.

In 2018, Lighthouse's Executive IT Director brought cybersecurity expert Bryan Seely on board to prevent costly system outages and ensure the infrastructure was secure and compliant with regulations when retrieving or communicating data with clients. *"I needed to troubleshoot recurring issues but had no visibility into the scope of public or private certificates across the company. It would have taken a year to manually discover the full extent of certificate inventory, as well as what was secure, active or needing renewal,"* **said Bryan Seely, Senior Systems Engineer, IT Security, Lighthouse Global.**

"With Sectigo Private PKI, you can connect to the network or the Microsoft agent and the software automatically populates the portal, so that you can manage all of your certificates from a single dashboard."

— Bryan Seely, Senior Systems Engineer, IT Security, Lighthouse Global

Certificate Manager Delivers Instant Visibility

Lighthouse explored building a solution and evaluated commercial options. Once the network team realized they could immediately issue SSL certificates for public web server infrastructure, as well as private, they felt there was no comparison to Sectigo Certificate Manager's visibility, efficiency or automation. The company purchased Certificate Manager, a variety of public SSL certificates, and premier customer support. Within weeks — using one platform to perform auto installations or renew web server certificates — the team was able to discover and log the status of every private certificate on its servers, devices, internal applications, clients (desktops, internal S/MIME email), and each public SSL certificate on its website.

Implementation was seamless, with Sectigo providing training calls and resources to ensure a smooth rollout. *"Installation of Sectigo certificates was about as easy as an enterprise deployment can be. The software installs with 5-6 clicks, allowing for a few self-explanatory options. It's also a forgiving reinstall. You don't have to go reboot the machine 25x and clear the registry history, praying you didn't break something in the process,"* explained Seely.

"The platform helped us find all the 'broken' certificates across our environment. Without Certificate Manager, it would be like trying to clean up your house, but it's too cluttered to even enter other rooms. Sectigo's scanning function works better than some of our own attempts at asset intelligence or event monitoring, which take much longer to configure and lack functionality. You can connect to the network or the Microsoft CA agent and the software automatically populates the portal, so you can manage all of your digital certificates from one dashboard," he added.

Private PKI Eases PKI Management

In early 2019, Lighthouse added Sectigo-hosted Private PKI, including a Lighthouse-branded offline root CA and Lighthouse-branded issuing CA, so that the team no longer had to maintain the PKI infrastructure and could easily scale the management of all certificates. Sectigo made the Private PKI available within two weeks so that Lighthouse could begin to deploy certificates throughout their enterprise, utilizing auto enrollment capabilities for Active Directory joint computers and workstations. Certificate Manager also provides a workflow for enrolling web server certificates from the Private PKI.

Lighthouse plans to deploy certificates to mobile devices for WiFi authentication using the Sectigo Private PKI. By integrating mobile device management with their SCEP endpoint and allowing Lighthouse to provision certificates to Mac OS, Android, and iOS devices, Private PKI enables the IT team to easily deploy 802.1x authentication, securing wired and wireless endpoints that need a certificate and touch the network.

Results That Scale

Using Sectigo solutions has saved the Lighthouse IT team significant time and enabled them to replace the organization's two-tier PKI infrastructure with Sectigo Certificate Manager. In late February 2019 alone, the Lighthouse IT team issued 10,000 certificates across the enterprise. Given success with Certificate Manager and Private PKI, in early 2019 Lighthouse began using Sectigo Code Signing certificates to ensure digital signing of the organization's powershell scripts.

The results and benefits of Sectigo enterprise solutions also extend to Lighthouse's clients. "We are an eDiscovery firm, so our customer base is companies dealing with alleged loss of data. Our infrastructure needs to be rock-solid. Sectigo is providing best-practice certificate discovery, and the foundation needed to deliver or implement other cybersecurity solutions. If you have crappy cabling, you won't have reliable lighting," explained Seely.

"People have to show ID when they go anywhere. Sectigo provides the best computer ID and reporting. It's invaluable to be able to scan everything quickly with help from people who have done this before at scale in complex environments. I will continue to explore other Sectigo products — I love the APIs and it's been great that the team continues to check on ways to help us past the deployment stage," he said.

About Sectigo

Sectigo (formerly Comodo CA) provides web security products that help customers protect, monitor, recover, and manage their web presence and connected devices. As the largest commercial Certificate Authority trusted by enterprises globally for more than 20 years, and more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape. For more information, visit www.sectigo.com.