cpl.thalesgroup.com

THALES
Building a future we can all trust

Let's Encrypt Powers New High-Volume Certificate Authority Service with Thales Luna HSMs

ISRG was founded to achieve a big goal: Accelerating the move to a world in which all web sites use encryption. To accomplish their vision and support their new 'Let's Encrypt' certificate authority, they needed hardware security modules (HSMs) that could secure private keys, while delivering optimized performance and reliability—so they chose Thales Luna Network HSMs.

The Organization

Based in California, Internet Security Research Group (ISRG) is a non-profit organization focused on reducing the financial, technological, and educational barriers that inhibit secure communication over the Internet. To fulfill this vision, the ISRG has launched Let's Encrypt, a new kind of certificate authority. Let's Encrypt has removed one of the most significant impediments to widespread adoption of encryption on the Web: the traditionally costly and complex process of getting and managing SSL certificates. Let's Encrypt is free to everyone, anywhere in the world, and is easy to use—people can be up and running with basic server certificates in less than a minute.

Challenge

When building their fully automated, freely available high-volume certificate authority, ISRG needed to establish an infrastructure that could scale, and scale rapidly.

Solution

With just two Luna Network HSM 1700s, ISRG was able to deliver a highly reliable certificate authority service to users while ensuring private keys remained secure at all times.

Benefit

Luna Network HSM appliances accommodated the scale the ISRG needed, even as they issued and maintained more than 12 million active certificates.

Let's Encrypt

> " We need three key things from our HSMs: security, stability, and performance. Security and stability are critical for meeting the expectations of our subscribers and maintaining our reputation as a trusted authority. Performance is critical for meeting strong demand while keeping costs down. We're currently delivering millions of new certificates per month, while continuing to support the more than 12 million active certificates we've already issued. With Luna Network HSM appliances, we've been able to reliably support this massive demand, while ensuring private keys stay secure."
>
> – Josh Aas, Executive Director, Internet Security Research Group

The Solution

"From the beginning, we knew we needed secure HSMs to protect the private keys we'd be generating, which is standard operating procedure for any certificate authority," stated Aas.

To protect their certificate authority system, the team at ISRG decided to leverage industry-leading Luna Network HSMs. As a general purpose HSM, Luna Network HSM can be easily integrated into a wide range of applications to accelerate cryptographic operations, secure the crypto key lifecycle, and acts a root of trust for your entire encryption infrastructure.

"We need three key things from our HSMs: security, stability, and performance. Security and stability are critical for meeting the expectations of our subscribers and maintaining our reputation as a trusted authority. Performance is critical for meeting strong demand while keeping costs down. We're currently delivering millions of new certificates per month, while continuing to support the more than 12 million active certificates we've already issued. With two Luna Network HSM appliances, we've been able to reliably support this massive demand, while ensuring private keys stay secure."

The Business Need

As we browse, bank, and shop online, it's become commonplace to see a padlock icon in our browser, indicating our communications with a site are encrypted. However, many web sites today still don't offer this level of protection. While Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), represent a ubiquitous standard for encrypting web traffic, certificates have been the main barrier to more widespread encryption adoption.

Certificates represent a foundational component of trust in our online world; they give site visitors the assurance that they're truly visiting the site they intended. The problem is that using certificates has been too costly and complex for many site operators, and certificates haven't been available at all in some parts of the world.

ISRG has set out to achieve a huge goal: getting to a point in which 100 percent of Web sites employ encryption. Through Let's Encrypt, ISRG aims to deliver all the certificates needed to make that happen, and that's a lot of certificates. Not only do millions of certificates need to be issued, but they need to be renewed every 60-90 days and have OCSP responses re-generated every 72 hours, so the work's never done. If that weren't enough, the ISRG isn't content to focus solely on web sites.

"We don't want to limit our services to web sites; we want to help support devices as well," explained Josh Aas, Executive Director, Internet Security Research Group. "When you consider the vast majority of homes in the U.S. have devices like routers and modems, and that virtually all have browser-based management interfaces that aren't secured, this is a major infrastructure issue. We're committed to delivering certificates to help secure these devices."

To support these goals, ISRG needed to implement a highly reliable, secure infrastructure that users could trust. The Let's Encrypt service is online and fully automated. Consequently, if any issues arose in the backend infrastructure, it could have a direct impact on the users' experience. Further, the ISRG needed to architect its environment in a way that would support rapid and massive growth. In establishing an environment to support these requirements, hardware security modules (HSMs) play an integral piece of the puzzle.

The Benefits

Luna Network HSM appliances have continued to deliver the high performance and responsiveness ISRG needed for its Let's Encrypt service, even as the service's adoption began to see explosive growth. Less than a year after launching, Let's Encrypt is now the world's largest certificate authority by issuance volume.

"Luna Network HSM appliances have been instrumental in supporting our rapid growth. They've helped ensure users have a positive experience working with the service, and they've continued to perform as needed as our volumes grew," Aas explained.

"Luna Network HSM appliances have enabled us to achieve our initial goals, and they leave us well positioned to accommodate our long-term plans. With our Luna Network HSM appliances, we anticipate that we will be able to support up to 250 million active certificates, enough to cover the vast majority, if not all, of the websites on the Internet."

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us