BLOG

Development, DevOps, Security

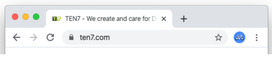
Why Are SSL Certificates Important?

Ivan Stegic — January 29, 2020

An SSL (Secure Sockets Layer) certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection. And your site needs one.

YE OLDE PADLOCK

Remember when ecommerce was starting to be a thing, and you'd get ready to buy something on the internet? You'd look at the URL to see if it said "https" instead of just "http." Or, you'd look for that little padlock next to the URL. The "s" in https means "secure."



A CRASH COURSE IN SSL CERTIFICATES

Tess Flynn, TEN7 DevOps Engineer, explains: "Let's say I (the web browser) show up at your door. I would like to talk to you (the website). I would like to use a secure channel to do that. We agree on a third party to mediate the conversation. That third party is represented by the SSL certificate."

With an SSL certificate in hand, the web browser checks it for authenticity, and then negotiates with the server on how best to encrypt any traffic between them. After this process, any communication remains encrypted using the agreed-upon protocols.

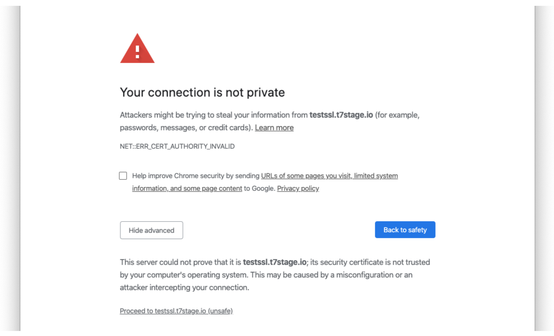
WHY SSL CERTIFICATES ARE CRUCIAL FOR SITE OWNERS

If a site isn't secure, data is not encrypted, and any text entered in a form—be it a credit card number, or a name and email in a contact form—is sent in plain text, and becomes susceptible to a "man-in-the-middle" attack. This can be a hacker on the other side of the world, or, if you're using an unsecured Wi-Fi network at a coffee shop, a guy next to you who has created a fake node on the public network and is grabbing any unencrypted data that comes across it.

Any site that enables the transfer of sensitive data (such as credit card information) should obviously be secured, but what about websites that are purely informative, like brochureware sites? "There's no good reason NOT to encrypt all web traffic," says Tess. "Even informational, non-login brochureware sites can pose a potential risk."

Let's use the example of a weather site. "You either enter your zip code to get the weather in your area, or you let the website geolocate you," says Tess. "Now you have the weather forecast, but the site also knows approximately where YOU are. A bad actor could use this information for nefarious purposes."

People have a higher expectation of security on the internet today, due to the frequency of site hacking. If visiting users don't see the "secure" symbols on a site, that could make them lose trust in the site and business. It's even worse if the site doesn't have an SSL certificate and users see this:



Another issue to be aware of is GDPR compliance. GDPR regulations don't mention SSL specifically, but they do have requirements that can only be addressed by SSL certificates.

There's a bigger problem to worry about if a site isn't secure: Google. In 2014, Google started including the presence of SSL certificates as a ranking factor. This means the site will get dinged in search results if it doesn't have a valid SSL certificate. And in 2018, Google started marking HTTP sites as "Not Secure" in the URL bar of its Chrome web browser.

THE CERTIFICATE AUTHORITY BUSINESS

So every site needs an SSL certificate. How do you get one? An SSL certificate must be obtained from a Certificate Authority (CA). A CA will verify details about a domain owner's request for an SSL certificate. If the information is valid, the CA will issue and "sign" the SSL certificate. The SSL certificate on the site is a part of a chain of certificates that begins with a "root" certificate at the CA level and ends with the SSL certificate on the website server. Trusted root status is only given to CAs that meet strict standards. Browsers and operating systems maintain a list of trusted CAs. If an SSL certificate is signed by one of these trusted CAs, it will also be trusted.

SSL certificates expire after a certain period and must be renewed. If an SSL certificate is found to have been compromised (mis-issued, or information from it stolen in a hack), it must be revoked and reissued.

In the past, being a Certificate Authority was quite lucrative. Every domain that wanted to be secure needed to pay for an SSL certificate, and if a site had subdomains, you either needed to get an SSL certificate for each one, or a "wild card" SSL certificate provisioned for the apex domain (such as "example.com" vs. "www.example.com") that would cover any subdomains (and usually this cost more than separate SSL certificates). People either forked over money directly to a CA, or they paid their hosting company a chunk of change to buy a certificate on their behalf. And there was plenty of money to be made on certificate renewal fees.

FREE CERTIFICATES

Then the nonprofit CA Let's Encrypt came along and changed that model. "Their view was, there's no reason why you can't use secure communication to browse ANY website," said Tess. "They thought that encrypting data is necessary because there are many ways we haven't even thought of yet that unencrypted data could be used maliciously." Let's Encrypt decided to provide certificates with a reasonable level of security (good enough for most people for most things) for FREE. What's it *not* good enough for, you might ask? Any site that requires an incredibly high security standard, like banks, credit card companies, the military, and so on. Over time, Let's Encrypt has become a de facto free SSL certificate provider.

In this era of "If a product is free, YOU'RE the product," why does Let's Encrypt give certificates for free? "Let's Encrypt is one of those weird companies that gives a damn about things," says Tess. "They're a project from the Internet Security Research Group (ISRG), a group that cares about privacy rights. If you're a person who cares about privacy and likes open source, you'll use Let's Encrypt."

MANAGING CERTIFICATES

Tracking and managing SSL certificates isn't necessarily hard, but it can be time-consuming, especially if you have multiple domains and/or subdomains on a site. Many CAs produce SSL certificates that expire after a year. With Let's Encrypt, it's three months. Some CAs will notify you before certificates expire, but some won't. Getting a new certificate is a manual process. You'll either have to pay the CA, or contact Let's Encrypt. You'll have to provision the new certificate, then revoke the old certificate, reboot the server, etc. Multiply all this work by however many domains or subdomains you have.

Many businesses don't have the necessary technical staff to do that, or they're paying the hosting provider to do that for them.

ARE YOU HOSTING WITH TEN7? THEN RELAX

If you're hosting with TEN7, managing and renewing SSL certificates isn't something you ever have to worry about. We take care of obtaining and provisioning SSL certificates from Let's Encrypt for your domains, and renewing them before they expire.

Our hosting, including the SSL certificate work, is all built on open source. Specifically, we now host clients using Flight Deck on Kubernetes at Digital Ocean. For SSL certificate provisioning and renewals, we're using an open source project called cert-manager that works with our Kubernetes-based hosting. Cert-manager automatically renews certificates after 60 days and transparently applies them to hosting infrastructure when complete. This way, a client hosted with TEN7 never has to worry about (or pay for!) a certificate again.

With your SSL certificates taken care of, your site visitors will feel safe, and you can take care of your business.

Would you like us to host your site? Contact us!

Ivan Stegic

CEO

Words that describe Ivan: Relentlessly optimistic. Kind. Equally concerned with client and employee happiness. Physicist. Ethical. Lighthearted and cheerful. Finds joy in the technical stuff. Inspiring. Loyal. Hires smart, curious and kind employees who want to create more good in the world.

BLOG POSTS

Case Studies

Case Study: Bloomington Public Schools - Drupal 8

Ivan Stegic — January 21, 2020

READ NOW

Case Studies

Case Study: Lutheran Social Service Of Minnesota Contact Directory

Ivan Stegic — December 6, 2019

READ NOW