FAQ

Archived: 2026-04-05 19:27:39 UTC

This FAQ is divided into the following sections:

General Questions

What services does Let's Encrypt offer?

Let's Encrypt is a global Certificate Authority (CA). We let people and organizations around the world obtain, renew, and manage SSL/TLS certificates. Our certificates can be used by websites to enable secure HTTPS connections.

Let's Encrypt offers Domain Validation (DV) certificates. We do not offer Organization Validation (OV) or Extended Validation (EV) primarily because we cannot automate issuance for those types of certificates.

To get started using Let's Encrypt, please visit our Getting Started page.

What does it cost to use Let's Encrypt? Is it really free?

We do not charge a fee for our certificates. Let's Encrypt is a nonprofit, our mission is to create a more secure and privacy-respecting Web by promoting the widespread adoption of HTTPS. Our services are free and easy to use so that every website can deploy HTTPS.

We require support from generous sponsors, grantmakers, and individuals in order to provide our services for free across the globe. If you're interested in supporting us please consider donating or becoming a sponsor.

In some cases, integrators (e.g. hosting providers) will charge a nominal fee that reflects the administrative and management costs they incur to provide Let's Encrypt certificates.

What kind of support do you offer?

Let's Encrypt is run by a small team and relies on automation to keep costs down. That being the case, we are not able to offer direct support to our subscribers. We do have some great support options though:

1. We have really helpful documentation.
2. We have very active and helpful community support forums. Members of our community do a great job of answering questions, and many of the most common questions have already been answered.

Here's a video we like about the power of great community support.

A website using Let's Encrypt is engaged in Phishing/Malware/Scam/… , what should I do?

We recommend reporting such sites to Google Safe Browsing and the Microsoft Smart Screen program, which are able to more effectively protect users. Here are the reporting URLs:

- https://safebrowsing.google.com/safebrowsing/report_badware/
- https://www.microsoft.com/en-us/wdsi/support/report-unsafe-site-guest

If you'd like to read more about our policies and rationale, you can do so here:

https://letsencrypt.org/2015/10/29/phishing-and-malware.html

Technical Questions

Are certificates from Let's Encrypt trusted by my browser?

For most browsers and operating systems, yes. See the compatibility list for more detail.

Does Let's Encrypt issue certificates for anything other than SSL/TLS for websites?

Let's Encrypt certificates are standard Domain Validation certificates, so you can use them for any server that uses a domain name, like web servers, mail servers, FTP servers, and many more.

Email encryption and code signing require a different type of certificate that Let's Encrypt does not issue.

Does Let's Encrypt generate or store the private keys for my certificates on Let's Encrypt's servers?

No. Never.

The private key is always generated and managed on your own servers, not by Let's Encrypt.

What is the lifetime for Let's Encrypt certificates? For how long are they valid?

Our default certificates are valid for 90 days. You can read about why here.

Subscribers can opt in to short-lived certificates which are valid for six days. You can read about these here.

There is no way to adjust these lifetimes, there are no exceptions. We recommend renewing 90 day certificates every 60 days and six day certificates every three days.

Will Let's Encrypt issue Organization Validation (OV) or Extended Validation (EV) certificates?

We have no plans to issue OV or EV certificates.

Can I get a certificate for multiple domain names (SAN certificates or UCC certificates)?

Yes, the same certificate can contain several different names using the Subject Alternative Name (SAN) mechanism.

Does Let's Encrypt issue wildcard certificates?

Yes. Wildcard issuance must use the DNS-01 challenge. See this post for more technical information.

Is there a Let's Encrypt (ACME) client for my operating system?

There are a large number of ACME clients available. Chances are something works well on your operating system. We recommend starting with Certbot.

Can I use an existing private key or Certificate Signing Request (CSR)?

Yes, but not all clients support this feature. Certbot does.

I requested a certificate and now my domain is receiving a lot of traffic! Why is this happening?

This is normal and anticipated. During the certificate issuance process, Let's Encrypt will validate control of your domain from multiple network perspectives. After successful validation, your certificate will be submitted to numerous Certificate Transparency (CT) logs. See here for more details about why this is necessary. Shortly after the certificate is submitted to CT, automated CT crawling bots will be able to discover your domain, attempt to access it, and generate further traffic in your webserver logs.

What IP addresses does Let's Encrypt use to validate my web server?

We don't publish a list of IP addresses we use to validate, and these IP addresses may change at any time. Note that we now validate from multiple IP addresses.

I successfully renewed a certificate but validation didn't happen this time - how is that possible?

Once you successfully complete the challenges for a domain, the resulting authorization is cached for your account to use again later. Cached authorizations last for up to 30 days from the time of validation, depending on the associated profile. If the certificate you requested has all of the necessary authorizations cached then validation will not happen again until the relevant cached authorizations expire.

Why should my Let's Encrypt (ACME) client run at a random time?

We ask that ACME clients perform routine renewals at random times to avoid spikes in traffic at set times of the day, such as exactly midnight UTC, or the first second of each hour or minute. When the service is too busy, clients will be asked to try again later, so randomizing renewal times can help avoid unnecessary retries.

Where can I learn more about TLS/SSL and PKI in general?

Longtime security researcher and practitioner, Ivan Ristić, published a configuration guide that provides useful information about what you should consider as you set up your TLS configuration.

For more extensive background and greater detail, we recommend Bulletproof TLS and PKI, also written by Ristić.
