

# Let's Encrypt

## info

- [User Guide](#)
- <https://letsencrypt.org/getting-started/>
- certbot
  - instalación: <https://certbot.eff.org/docs/install.html>
  - método manual: <https://certbot.eff.org/docs/using.html#manual>
  - renovación:
    - <https://certbot.eff.org/docs/using.html#re-creating-and-updating-existing-certificates>
    - ? <https://certbot.eff.org/docs/using.html#id19>
  - cli : <https://certbot.eff.org/docs/using.html#certbot-command-line-options>
- <https://www.adictosaltrabajo.com/2016/07/21/obtencion-de-certificados-con-lets-encrypt/>

## install

```
sudo apt install software-properties-common
sudo add-apt-repository universe
sudo apt update

sudo apt install certbot
```

+ info: <https://eff-certbot.readthedocs.io/en/stable/install.html>

## user guide

- <https://eff-certbot.readthedocs.io/en/stable/using.html>
- <https://certbot.eff.org/>

## standalone (no webserver)

```
sudo certbot certonly --standalone --agree-tos --email sammy@your_domain -d
<DOMAIN>
sudo certbot renew [--dry-run]
# programaticamente si hay que parar servicios:
# --pre-hook "service haproxy stop" --post-hook "service haproxy start"

# dejará los certificados del dominio en /etc/letsencrypt/live/<DOMAIN>/
```

obtener los certificados de Let's Encrypt:

```
curl -s
https://letsencrypt.org/certs/{isrgrootx1.pem.txt,letsencryptauthorityx3.pem.txt} >
~/letsencrypt-combined-certs.pem
sudo cp ~/letsencrypt-combined-certs.pem /etc/letsencrypt/live/your_domain/
```

/via: <https://certbot.eff.org/lets-encrypt/debianbuster-other>

/via: <https://certbot.eff.org/instructions>

## DNS challenge

Este método te exige poner una clave TXT en tu servidor DNS para certificar que puedes acceder a ese dominio:

```
sudo ./certbot-auto --manual --preferred-challenge dns certonly --email sammy@your_domain -d seedbox.torresegea.es
```

si todo está correcto, te genera 3 ficheros (/etc/letsencrypt/live/<dominio>), que corresponden a las líneas de configuración de apache correspondientes:

- cert.pem → SSLCertificateFile
- chain.pem → SSLCertificateKeyFile
- privkey.pem → SSLCACertificateFile

Existen otros métodos (explicados en documentación) para validar un dominio

## comandos

- sudo ./certbot-auto --help all
- sudo ./certbot-auto certificates: listado de certificados
- sudo ./certbot-auto certonly -d <dominio>: renovación manual certificado

## ejemplos

- [nginx+certbot en contenedor](#)
- [let's encrypt k0.vividumcodex.com](#)
- [let's encrypt seedbox.torresegea.es](#)
- [Let's Encrypt multidominio](#)

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/web:security:letsencrypt?rev=1651472819>

Last update: **01/05/2022 23:26**

