Let's Encrypt

info

- User Guide
- https://letsencrypt.org/getting-started/
- https://www.adictosaltrabajo.com/2016/07/21/obtencion-de-certificados-con-lets-encrypt/

certbot

- 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

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

comandos

- listado de certicados:

  ```
  sudo certbot certificates
  ```

- renovación manual certificado:

  ```
  sudo certbot certonly --manual --preferred-challenges=dns --email
  informatica@fidmag.org --server https://acme-v02.api.letsencrypt.org/directory
  --agree-tos -d *.fidmag.org
  ```

- borrado:

  ```
  sudo certbot delete --cert-name <CERT_NAME>
  ```

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>/
```

certificados Let's encrypt

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

La renovación implica usar un servicio DNS que permita actualizar los registros a través de una API o delegar en uno que sí lo permita: Let's Encrypt (renovación DNS)

webroot

```
sudo mkdir -p /var/www/letsencrypt/.well-known/acme-challenge
sudo chown -R www-data:www-data /var/www/letsencrypt
```

```
<VirtualHost *:80>
        ServerName xxx.org
        DocumentRoot /var/xxx/html
        Alias /.well-known/acme-challenge/ /var/www/letsencrypt/.well-known/acme-
```

```
challenge/

        <Directory /var/www/letsencrypt/>
                AllowOverride None
                Require all granted
        </Directory>

        RewriteEngine On
        RewriteCond %{REQUEST_URI} !^/\.well-known [NC]
        RewriteRule ^(.*)$ https://fidmag.org/ca/xxx.html [L,R=301]
</VirtualHost>
```

```
sudo /usr/bin/certbot certonly --webroot -w /var/www/letsencrypt --agree-tos --
email informatica@xxx.org -d xxx.org
```

ejemplos

- Let's encrypt k0.vividumcodex.com mate
- Let's Encrypt multidominio mate
- Let's encrypt seedbox.torresegea.es mate
- Let's Encrypt wildcard mate
- nginx+certbot en contenedor mate