Está claro que cada vez más, es imprescindible tener un certificado firmado (y no autofirmado) sobre todo para dar servicio, fuera de nuestras pruebas internas.

letsencrypt una autoridad de certificación, nos ayuda con esta labor y nos proporciona éste servicio de **forma gratuita**.

Cerbot, será el software encargado de gestionar los certificados de nuestra máquina; ya sea de forma local (sin ser frontal de apache) o siendo un proxy de las peticiones http.

En **Debian**/**Ubuntu** haremos lo siguiente:

1) Prepararemos el sistema para instalar Certbot

```
$ sudo apt-get update
$ sudo apt-get install software-properties-common
$ sudo add-apt-repository universe
$ sudo add-apt-repository ppa:certbot/certbot
$ sudo apt-get update
```

2) Realizaremos la instalación

```
$ sudo apt-get install certbot python-certbot-apache
```

3) En principio con el siguiente comando, Certbot incluiría en todos vuestros hosts o virtualhosts de apache los certificados firmados sin que tuvierais que hacer nada más, aunque en mi caso y usando proxypass, fue necesario, usar el comando del paso 4)

```
$ sudo certbot --apache
```

4) Comando, que tuve que usar en mi frontal de apache, para dar de alta un site con el certificado firmado por letsencrypt

```
$ sudo letsencrypt --apache -d webservice.acabey.xyz
```

5) Aunque Certbot modificará una línea (probablemente /etc/cron.d/certbot) para realizar la comprobación de caducidad de los certificados; con éste comando, podréis verificarlo a mano

```
$ sudo certbot renew --dry-run
```