Let's Encrypt (renovación DNS)

Para poder renovar los certificados a través DNS, hace falta usar un servicio que permita acceder a los registros DNS via API (o delegar el registro CNAME en uno que lo permita).

preparativos

- descargar el script encargado de modificar el registro DNS:

```
sudo curl -o /etc/letsencrypt/acme-dns-auth.py
https://raw.githubusercontent.com/joohoi/acme-dns-certbot-joohoi/master/acme-dns-auth.py
sudo chmod +x /etc/letsencrypt/acme-dns-auth.py
```

- Asegurarse de que apunte a la versión de Python del sistema **#!/usr/bin/env python3**
  - `apt install python-is-python3`

primera configuración

- Ejecutar

```
sudo certbot certonly --manual --manual-auth-hook /etc/letsencrypt/acme-dns-auth.py --preferred-challenges dns --debug-challenges -d "*.fidmag.org" -d "fidmag.org"
```

  - guardará credenciales de **auth.acme-dns.io** en **/etc/letsencrypt/acmedns.json**
  - la primera vez se creará el registro en **auth.acme-dns.io**
    - importante anotar el valor obtenido
  - hay que indicar en el registro CNAME **_acme-challenge** el código anterior. Esto indicará que ese registro está delegado. Esperar a la propagación, verificar usando:
    - https://toolbox.googleapps.com/apps/dig/#TXT/_acme-challenge.fidmag.org
    - https://www.whatsmydns.net/#TXT/_acme-challenge.fidmag.org

```
dig _acme-challenge.fidmag.org CNAME +short
```

renovaciones

```
certbot renew --post-hook "systemctl reload nginx" (o apache2)
```

```
certbot renew --post-hook "docker compose -f /home/fidmag/webservices/docker-compose.yml restart"
```

Después copiar los certificados donde correspondan

```
# execució manual
sudo certbot certonly --manual \
    --manual-auth-hook /etc/letsencrypt/acme-dns-auth.py \
    --preferred-challenges dns \
    --debug-challenges \
```

```
    -d "fidmag.org" \
    -d "*.fidmag.org"

[[ $? -eq 0 ]] && {
    echo "Renovación exitosa. Actualizando certificados en webservices..."

    # Ejecutamos en cadena (&&): si un paso falla, se detiene para no romper nada
    sudo mv -f /home/fidmag/webservices/certs/fullchain.pem
/home/fidmag/webservices/certs/fullchain.pem.old && \
    sudo mv -f /home/fidmag/webservices/certs/fullchain.pem.key
/home/fidmag/webservices/certs/fullchain.pem.key.old && \
    sudo cp -f /etc/letsencrypt/live/fidmag.org/fullchain.pem
/home/fidmag/webservices/certs/ && \
    sudo cp -f /etc/letsencrypt/live/fidmag.org/privkey.pem
/home/fidmag/webservices/certs/fullchain.pem.key && \
    sudo chmod +r /home/fidmag/webservices/certs/* && \

    docker compose -f /home/fidmag/webservices/docker-compose.yml restart
}
```

opción manual

```
sudo certbot certonly --manual --preferred-challenges dns -d "*.fidmag.org" -d
"fidmag.org"
```

Después copiar los certificados donde correspondan

From:
https://matebcn.eu/ - **miguel angel torres egea**

Permanent link:
https://matebcn.eu/web:security:letsencrypt:dns

Last update: **01/06/2026 11:27**