# openssl

- Certificados, certificaciones, Entidades de Certificación
- https://www.sslshopper.com/article-most-common-openssl-commands.html

## utils

- Remove a passphrase from a private key:

```
openssl rsa -in privateKey.pem -out newPrivateKey.pem
```

## check

- Check a Certificate Signing Request (CSR):

```
openssl req -text -noout -verify -in CSR.csr
```

- Check a private key:

```
openssl rsa -in privateKey.key -check
```

- Check a certificate:

```
openssl x509 -in certificate.crt -text -noout
```

- Check a PKCS#12 file (.pfx or .p12):

```
openssl pkcs12 -info -in keyStore.p12
```

## debug

- Check an MD5 hash of the public key to ensure that it matches with what is in a CSR or private key:

```
openssl x509 -noout -modulus -in certificate.crt | openssl md5
openssl rsa -noout -modulus -in privateKey.key | openssl md5
openssl req -noout -modulus -in CSR.csr | openssl md5
```

## converting

- Convert a DER file (.crt .cer .der) to PEM:

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

- Convert a PEM file to DER:

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

- Convert a PKCS#12 file (.pfx .p12) containing a private key and certificates to PEM:

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

- Convert a PEM certificate file and a private key to PKCS#12 (.pfx .p12):

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
certificate.crt -certfile CACert.crt
```

## pfx

verificar dades del certificat:

```
openssl pkcs12 -in certificado.pfx -nokeys | openssl x509 -noout -enddate
```

```
openssl pkcs12 -in certificado.pfx -nokeys | openssl x509 -noout -dates
```

```
openssl pkcs12 -in certificado.pfx -nokeys | openssl x509 -noout -text
```

## generar PFX desde PEM

```
#! /usr/bin/env bash

sudo openssl pkcs12 -export \
    -out /home/fidmag/certbot/fidmag.org.pfx \
    -inkey /etc/letsencrypt/live/fidmag.org/privkey.pem \
    -in /etc/letsencrypt/live/fidmag.org/fullchain.pem \
    --passout pass:password
sudo chown fidmag /home/fidmag/certbot/fidmag.org.pfx
```

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

Permanent link:
**https://matebcn.eu/web:security:openssl**

Last update: **17/09/2026 10:32**