# Un documento firmado, y cómo se firmó

Este archivo lleva una firma digital. Cubre cada byte del archivo
salvo el lugar donde está escrita: un byte cambiado en cualquier sitio la rompe, y
el programa de lectura lo dice.

El certificado es de demostración: se hizo para este ejemplo,
y no nombra a ninguna persona ni empresa. La firma prueba que el archivo
no ha cambiado; no prueba nada de quién lo firmó, porque nadie
responde de este certificado.




## Cómo se firmó

1. La clave y su certificado se hicieron una vez, desde la raíz del repositorio:

```
openssl req -x509 -newkey rsa:2048 -nodes -days 3650
    -subj "/CN=hqf-pdf demonstration signer"
    -keyout keys/demonstration_signer.key -out keys/demonstration_signer.crt
```

2. La biblioteca recibe el certificado en DER, que escribe esto:

```
openssl x509 -in keys/demonstration_signer.crt -outform DER
```

3. La biblioteca deja sitio en el archivo para la firma, calcula el resumen
de cada byte a su alrededor y pasa al programa los atributos que firmar.
La clave los firma, y nunca llega a la biblioteca:

```
openssl dgst -sha256 -sign keys/demonstration_signer.key
```

4. La biblioteca envuelve esa firma y el certificado en la estructura
que lleva una firma PAdES, y la escribe en el sitio que dejó.

## Comprobarla sin esta biblioteca

El /ByteRange del archivo nombra los dos tramos de bytes que cubre la firma,
y /Contents guarda la estructura entre ellos, en hexadecimal. Concatene
los dos tramos en covered.bin, decodifique la estructura en signature.der,
y ejecute:

```
openssl cms -verify -binary -inform DER -in signature.der -content covered.bin
    -CAfile keys/demonstration_signer.crt -purpose any
```