Um documento assinado, e como foi assinado

Este ficheiro leva uma assinatura digital. Cobre cada byte do ficheiro
exceto o lugar onde está escrita: um byte mudado em qualquer sítio parte-a, e
o programa de leitura di-lo.

O certificado é de demonstração: foi feito para este exemplo,
e não nomeia nenhuma pessoa nem empresa. A assinatura prova que o ficheiro
não mudou; não prova nada sobre quem o assinou, porque ninguém
responde por este certificado.



Como foi assinado

1. A chave e o seu certificado foram feitos uma vez, a partir da raiz do repositório:

```
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. A biblioteca recebe o certificado em DER, que este comando escreve:

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

3. A biblioteca deixa espaço no ficheiro para a assinatura, calcula o resumo
de cada byte à volta e passa ao programa os atributos a assinar.
A chave assina-os, e nunca chega à biblioteca:

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

4. A biblioteca embrulha essa assinatura e o certificado na estrutura
que uma assinatura PAdES leva, e escreve-a no espaço que deixou.

Verificá-la sem esta biblioteca

O /ByteRange do ficheiro nomeia os dois troços de bytes que a assinatura cobre,
e /Contents guarda a estrutura entre eles, em hexadecimal. Junte
os dois troços em covered.bin, descodifique a estrutura em signature.der,
e execute:

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