Un documento firmato, e come è stato firmato

Questo file porta una firma digitale. Copre ogni byte del file tranne il punto in cui è scritta: un byte cambiato ovunque la rompe, e il programma di lettura lo dice.

Il certificato è di dimostrazione: è stato fatto per questo esempio, e non nomina nessuna persona né azienda. La firma prova che il file non è cambiato; non prova nulla su chi l'ha firmato, perché nessuno garantisce per questo certificato.



Come è stato firmato

1. La chiave e il suo certificato sono stati fatti una volta, dalla radice del repository:

```
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 libreria riceve il certificato in DER, che scrive questo:

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

3. La libreria lascia spazio nel file per la firma, calcola l'impronta di ogni byte intorno e passa al programma gli attributi da firmare. La chiave li firma, e non arriva mai alla libreria:

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

4. La libreria avvolge quella firma e il certificato nella struttura che porta una firma PAdES, e la scrive nello spazio lasciato.

Verificarla senza questa libreria

Il /ByteRange del file nomina i due tratti di byte che la firma copre, e /Contents tiene la struttura tra di essi, in esadecimale. Unite i due tratti in covered.bin, decodificate la struttura in signature.der, ed eseguite:

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