Un document signé, et comment il l'a été

Ce fichier porte une signature numérique. Elle couvre chaque octet du fichier sauf la place où elle est écrite : un seul octet changé, où que ce soit, la rompt, et le logiciel de lecture le dit.

Le certificat est un certificat de démonstration : il a été fait pour cet exemple, et il ne nomme ni personne ni entreprise. La signature prouve que le fichier n'a pas changé ; elle ne prouve rien de qui l'a signé, puisque personne ne se porte garant de ce certificat.

hqf-pdf demonstration signer
Signé le 2026-09-13 08:00 UTC

Comment il a été signé

1. La clé et son certificat ont été faits une fois, depuis la racine du dépôt :

```
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 bibliothèque reçoit le certificat en DER, que ceci écrit :

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

3. La bibliothèque laisse dans le fichier la place de la signature, calcule l'empreinte de chaque octet autour, et donne au programme les attributs à signer. La clé les signe, et n'entre jamais dans la bibliothèque :

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

4. La bibliothèque enveloppe cette signature et le certificat dans la structure qu'une signature PAdES porte, et l'écrit dans la place laissée.

Le vérifier sans cette bibliothèque

Le /ByteRange du fichier nomme les deux plages d'octets que la signature couvre, et /Contents contient la structure entre elles, en hexadécimal. Joignez les deux plages dans covered.bin, décodez la structure dans signature.der, puis lancez :

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