Un document signé, et comment il l’a été

Ce fichier contient une signature numérique. Elle couvre chaque octet du fichier, sauf l’endroit où elle est écrite : un seul octet modifié, où que ce soit, la rompt, et le logiciel de lecture le signale.

Le certificat est un certificat de démonstration : il a été créé pour cet exemple, et ne nomme ni personne ni entreprise. La signature prouve que le fichier n’a pas changé ; elle ne dit rien de l’identité du signataire, puisque personne ne se porte garant de ce certificat.



Comment il a été signé

1. La clé et son certificat ont été générés 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, produit par cette commande :

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

3. La bibliothèque réserve dans le fichier la place de la signature, calcule l’empreinte de tous les octets autour, et remet au programme les attributs à signer. La clé les signe sans jamais entrer dans la bibliothèque :

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

4. La bibliothèque enveloppe cette signature et le certificat dans la structure que prévoit une signature PAdES, et l’écrit dans la place réservée.

Le vérifier sans cette bibliothèque

Le /ByteRange du fichier désigne les deux plages d’octets que la signature couvre, et /Contents contient la structure placée entre elles, en hexadécimal. Concaténez 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
```