Un fichier reçu, puis signé deux fois

Cette page tient lieu d’un fichier envoyé par quelqu’un d’autre. Il a d’abord été écrit seul, sans formulaire ni place pour signer ; les deux cadres ci-dessous y ont été ajoutés ensuite, sans déplacer un seul octet.

Les deux signatures sont faites avec la clé de démonstration du dossier keys/ : elles prouvent que les octets n’ont pas changé, et rien sur le signataire.

Chaque cadre est entré dans une section ajoutée après le dernier octet. Puis l’approbation a été signée, et la relecture après elle, chacune dans sa propre section, elle aussi. La relecture couvre tout le fichier ; l’approbation couvre exactement les octets couverts à sa création, et se vérifie toujours.

Approbation

Relecture

Les vérifier toutes deux sans cette bibliothèque

Le fichier contient un /ByteRange par signature. Pour chacun, concaténez ses deux plages dans covered.bin, décodez la structure entre elles dans signature.der, puis lancez :

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

Enfin, une cinquième section conserve le certificat de démonstration, pour les deux signatures, dans le magasin de sécurité du fichier : elles resteront vérifiables.