

Un archivo recibido, y luego firmado dos veces

Esta página representa un archivo que envió otra persona. Se escribió primero, solo, sin formulario ni lugar para firmar; las dos cajas enmarcadas de abajo se le añadieron después, y ni uno de sus bytes se ha movido.

Las dos firmas se hacen con la clave de demostración guardada en keys/: prueban que los bytes no cambiaron, y no prueban nada de quién las firmó.

Cada caja entró como una sección añadida tras el último byte del archivo. Luego se firmó la aprobación, y la revisión después, cada una otra vez en una sección propia. La revisión cubre el archivo entero; la aprobación sigue cubriendo exactamente los bytes que cubría al hacerse, y sigue verificándose.

Aprobación

Revisión

Comprobar las dos sin esta biblioteca

El archivo tiene un /ByteRange por firma. Para cada una, concatene sus dos tramos en covered.bin, decodifique la estructura entre ellos en signature.der, y ejecute:

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

Por último, una quinta sección guarda el certificado de demostración en el almacén de seguridad, para que ambas firmas sigan siendo verificables.