

Un file ricevuto, poi firmato due volte

Questa pagina rappresenta un file inviato da qualcun altro. È stato scritto prima, da solo, senza modulo né posto per firmare; i due riquadri incorniciati qui sotto gli sono stati aggiunti dopo, e nemmeno uno dei suoi byte si è mosso.

Entrambe le firme sono fatte con la chiave di dimostrazione registrata in keys/: provano che i byte non sono cambiati, e nulla su chi li ha firmati.

Ogni riquadro è entrato come una sezione aggiunta dopo l'ultimo byte del file. Poi è stata firmata l'approvazione, poi la revisione, ciascuna di nuovo in una sezione propria. La revisione copre l'intero file; l'approvazione copre ancora esattamente i byte che copriva quando è stata fatta, e si verifica ancora.

Approvazione



Revisione



Verificarle entrambe senza questa libreria

Il file ha un /ByteRange per firma. Per ciascuna, unite i suoi due tratti in covered.bin, decodificate la struttura tra di essi in signature.der, ed eseguite:

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

Infine, una quinta sezione conserva il certificato di dimostrazione nell'archivio di sicurezza, perché entrambe le firme restino verificabili.