

Een ontvangen bestand, tweemaal ondertekend

Deze pagina staat voor een bestand van iemand anders. Het is eerst geschreven, op zichzelf, zonder formulier of tekenplek; de twee omkaderde vakken hieronder zijn er later aan toegevoegd, en geen enkele byte ervan is verschoven.

Beide handtekeningen zijn gemaakt met de demonstratiesleutel in keys/: ze bewijzen dat de bytes niet veranderd zijn, en niets over wie tekende.

Elk vak kwam erin als een sectie na de laatste byte van het bestand. Daarna werd de goedkeuring ondertekend, en de beoordeling erna, elk weer in een eigen sectie. De beoordeling dekt het hele bestand; de goedkeuring dekt nog steeds precies de bytes die ze dekte toen ze gezet werd, en klopt nog steeds.

Goedkeuring

Beoordeling

Beide controleren zonder deze bibliotheek

Per handtekening is er één /ByteRange. Voeg voor elk de twee reeksen samen tot covered.bin, decodeer de structuur ertussen naar signature.der, en voer uit:

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

Ten slotte bewaart een vijfde sectie het demonstratiecertificaat in de beveiligingsopslag, zodat beide handtekeningen later te controleren blijven.