

Um ficheiro recebido, depois assinado duas vezes

Esta página faz as vezes de um ficheiro que alguém enviou. Foi escrito primeiro, sozinho, sem formulário nem lugar para assinar; as duas caixas emolduradas abaixo foram-lhe acrescentadas depois, e nem um dos seus bytes se mexeu.

As duas assinaturas são feitas com a chave de demonstração guardada em keys/: provam que os bytes não mudaram, e nada sobre quem os assinou.

Cada caixa entrou numa secção acrescentada após o último byte do ficheiro. Depois foi assinada a aprovação, e a revisão a seguir, cada uma de novo numa secção própria. A revisão cobre o ficheiro inteiro; a aprovação continua a cobrir exatamente os bytes que cobria quando foi feita, e continua a verificar-se.

Aprovação

Revisão

Verificar as duas sem esta biblioteca

O ficheiro tem um /ByteRange por assinatura. Para cada uma, junte os dois troços em covered.bin, descodifique a estrutura entre eles em signature.der, e execute:

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

Por fim, uma quinta secção guarda o certificado de demonstração no arquivo de segurança, para as duas assinaturas continuarem verificáveis.