

Eine erhaltene Datei, dann zweimal signiert

Diese Seite steht für eine Datei, die jemand anderes schickte. Sie entstand zuerst für sich, ohne Formular und ohne Unterschriftsfeld; die beiden Kästen unten kamen danach hinzu, und kein einziges ihrer Bytes hat sich verändert.

Beide Signaturen stammen vom Vorführschlüssel aus keys/: Sie beweisen, dass die Bytes unverändert sind, und nichts über die Unterzeichner.

Jeder Kasten kam als Abschnitt hinter das letzte Byte der Datei. Dann wurde die Freigabe signiert, danach die Prüfung, jede wieder in einem eigenen Abschnitt. Die Prüfung deckt die ganze Datei ab; die Freigabe deckt noch genau die Bytes von damals und lässt sich weiterhin verifizieren.

Freigabe

Prüfung

Beide ohne diese Bibliothek prüfen

Die Datei enthält je Signatur ein /ByteRange. Für jede die zwei Folgen zu covered.bin zusammenfügen, die Struktur dazwischen zu signature.der dekodieren und ausführen:

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

Zuletzt legt ein fünfter Abschnitt das Vorführzertifikat im Sicherheitsspeicher der Datei ab, damit beide Signaturen prüfbar bleiben.