Ein signiertes Dokument und seine Signatur

Diese Datei trägt eine digitale Signatur. Sie deckt jedes Byte ab,
außer der Stelle, an der sie steht: Ein geändertes Byte irgendwo bricht sie,
und die Lesesoftware sagt es.

Das Zertifikat ist ein Vorführzertifikat, für dieses Beispiel erstellt,
und nennt weder Person noch Firma. Die Signatur beweist, dass die Datei
unverändert ist; über den Unterzeichner beweist sie nichts, denn niemand
bürgt für dieses Zertifikat.



Wie es signiert wurde

1. Schlüssel und Zertifikat, einmal im Wurzelordner des Repositorys erstellt:

```
openssl req -x509 -newkey rsa:2048 -nodes -days 3650
   -subj "/CN=hqf-pdf demonstration signer"
   -keyout keys/demonstration_signer.key -out keys/demonstration_signer.crt
```

2. Die Bibliothek erhält das Zertifikat als DER, geschrieben so:

```
openssl x509 -in keys/demonstration_signer.crt -outform DER
```

3. Die Bibliothek lässt Platz für die Signatur, bildet den Hashwert
aller Bytes ringsum und übergibt dem Programm die zu signierenden Attribute.
Der Schlüssel signiert sie und erreicht die Bibliothek nie:

```
openssl dgst -sha256 -sign keys/demonstration_signer.key
```

4. Die Bibliothek verpackt diese Signatur und das Zertifikat in die Struktur
einer PAdES-Signatur und schreibt sie in den freigelassenen Platz.

Prüfung ohne diese Bibliothek

/ByteRange nennt die zwei Bytefolgen, die die Signatur abdeckt,
und /Contents enthält die Struktur dazwischen, hexadezimal. Die beiden Folgen
zu covered.bin zusammenfügen, die Struktur 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
```