A file received, then signed twice

This page stands for a file somebody else sent. It was written first, on its own, with no form and no place to sign; the two framed boxes below were added to it afterwards, and not one of its bytes has moved.

Both signatures are made with the demonstration key committed in keys/: they prove the bytes unchanged, and nothing about who signed them.

Each box went in as a section appended after the file's last byte. Then the approval was signed, and the review after it, each in a section of its own again. The review covers the whole file; the approval still covers exactly the bytes it covered when it was made, and still verifies.

Approval

Review

Checking both without this library

The file holds one /ByteRange per signature. For each, join its two runs into covered.bin, decode the structure between them into signature.der, and run:

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

Last, a fifth section keeps the demonstration certificate in the file's security store, filed under both signatures, so both stay checkable later.