The same signature, made in two stages

The document beside this one was signed while it was being written. This one was not: it left tclpdf with the placeholder still in it, and the signature was put in afterwards. That is the way that matters in practice, because the key is usually not in the process that writes the document - it is on a card in a reader, in an HSM, or behind a signing service.

What it proves, and what it does not

It proves two things. The bytes /ByteRange names have not changed since they were signed, and whoever signed them held the private key belonging to the certificate inside the CMS object. It proves nothing at all about WHO that was. That answer comes from the certificate chain, and only if the issuer at the end of it is one the reader already trusts.

And the caveat from the other page holds here too: the issuer is a test CA that was generated a moment before this document, in a temporary directory, and deleted a moment after. Every reader will report it as untrusted, and that is the correct answer, not a defect in the file.

Check it yourself

```
pdfsig 08.01-signature-two-stage.pdf
qpdf --check 08.01-signature-two-stage.pdf
pdfsig -dump 08.01-signature-two-stage.pdf
openssl cms -verify -inform DER -in 08.01-signature-two-stage.pdf.sig0 \
    -content bytes.bin -binary -noverify
```