A signed document

This file carries a digital signature, and what that means in a PDF is narrower than the word suggests. A dictionary in the file names a range of bytes and stores a CMS object made over exactly those bytes. If one byte inside the range changes afterwards, the digest no longer matches, and every reader that looks says so.

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.

This document is signed by a test CA that was generated a moment before it, in a temporary directory, and deleted a moment after. Every reader will report the issuer as untrusted - and that is the correct answer, not a defect in the file. A valid signature and a trusted signature are two different statements, and only the first one is a question about the PDF.

Check it yourself

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