Signed, then stamped

This file answers two different questions with two different mechanisms. The signature says WHO: a CMS object over the bytes /ByteRange names, made with the signer's key, verifiable against the signer's certificate. The document timestamp says SINCE WHEN: an RFC 3161 token over every byte of the signed file, made with a timestamp authority's key, verifiable against the authority's chain.

Why the order matters

The stamp was appended after the signature, so its range covers the signature itself. The token therefore fixes the moment by which the signature existed - which is what keeps the signature provable after the signer's certificate expires. That is the base pattern of long-term validation, and further stamps may follow years apart, each covering everything before it.

Check it yourself

```
pdfsig 08.08-signature-doctimestamp.pdf
qpdf --check 08.08-signature-doctimestamp.pdf
pdfsig -dump 08.08-signature-doctimestamp.pdf
```