



Web



Signature lifecycle



WEB > GUIDES > PSPDFKIT SERVER > DIGITAL SIGNATURES > SIGNATURE LIFECYCLE

Ensure effective digital signature validation



PSPDFKit Server has been deprecated and replaced by [Document Engine](#). To migrate to Document Engine and unlock advanced document processing capabilities, refer to our [migration guide](#). Learn more about these enhancements on our [blog](#).

The digital signature validation process consists of two steps.

- ❖ In the first step, it checks if the signature certificate embedded during signing can be trusted. To do this, the trusted certificate chain up to the root authority that issued it is necessary. Nutrient Web SDK with and without Document Engine both allow you to specify the certificates to use for validation.
- ❖ In the second step, it verifies the signature. This process essentially applies the public key (from the certificate embedded in the PDF file) to the digital signature and compares the result with the message digest built from the PDF file, excluding the signature itself. If the result is the same, the signature is valid.

Providing trusted root certificates

PSPDFKit Server will search for certificate stores at the `/certificate-stores` path inside its container. You can mount a folder from the host machine containing your certificates. As an example, you can update the configuration in the Docker Compose file by adding the needed volume:

```
1 pspdfkit:
2 ...
```



ASK AI

```
3 volumes:
4   - "/path-on-the-host:/certificate-stores"
```

Note that for performance reasons, PSPDFKit Server defers loading certificate files until a signature needs to be validated, so you'll need to open a signed document to test that the files are loaded as expected.

Was this helpful?

✓ YES

✗ NO

Questions? [Contact us](#)

