# Validating Digital Signatures in Adobe Reader

- Usually, the digital certificates are issued by a Root CA (Certification Authority).

- If the Root CA certificate is not included in Adobe Trusted Identities, the digital signature is considered "not trusted" (but NOT invalid) when the document is opened in Adobe Reader (**see example below**).

- As an alternative, the user must manually add the Root Certificate of the signing certificate on Adobe because only a few Root CA's are considered trusted by default by the Adobe certificate validation engine.

Adding the Root Certificate on Adobe Trusted Identities:

- **Click on rectangular signature in the pdf**
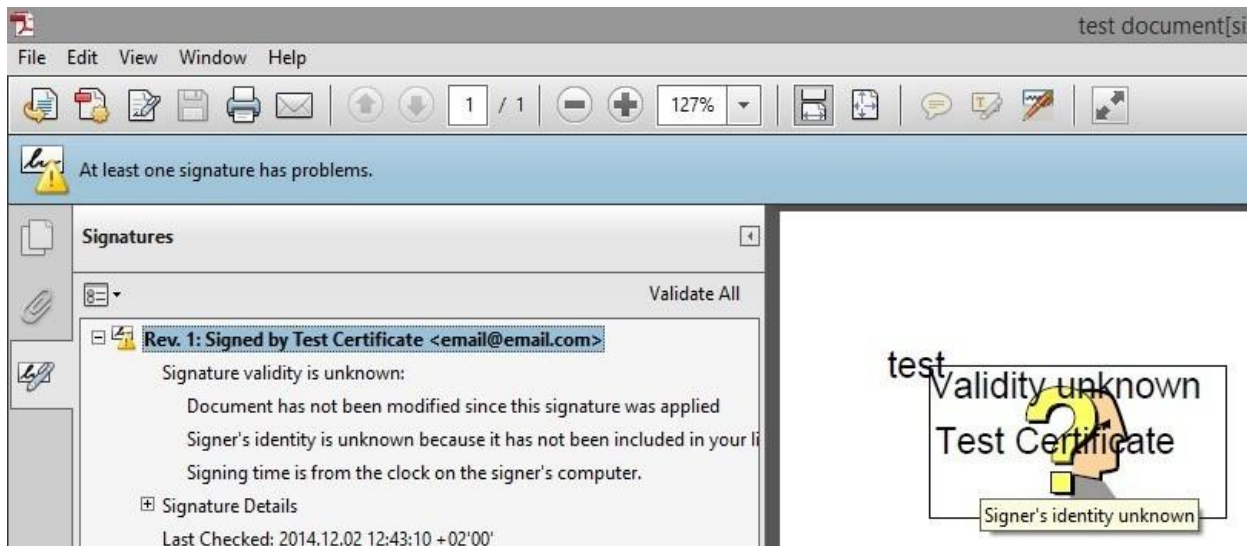
The digital signature in not trusted
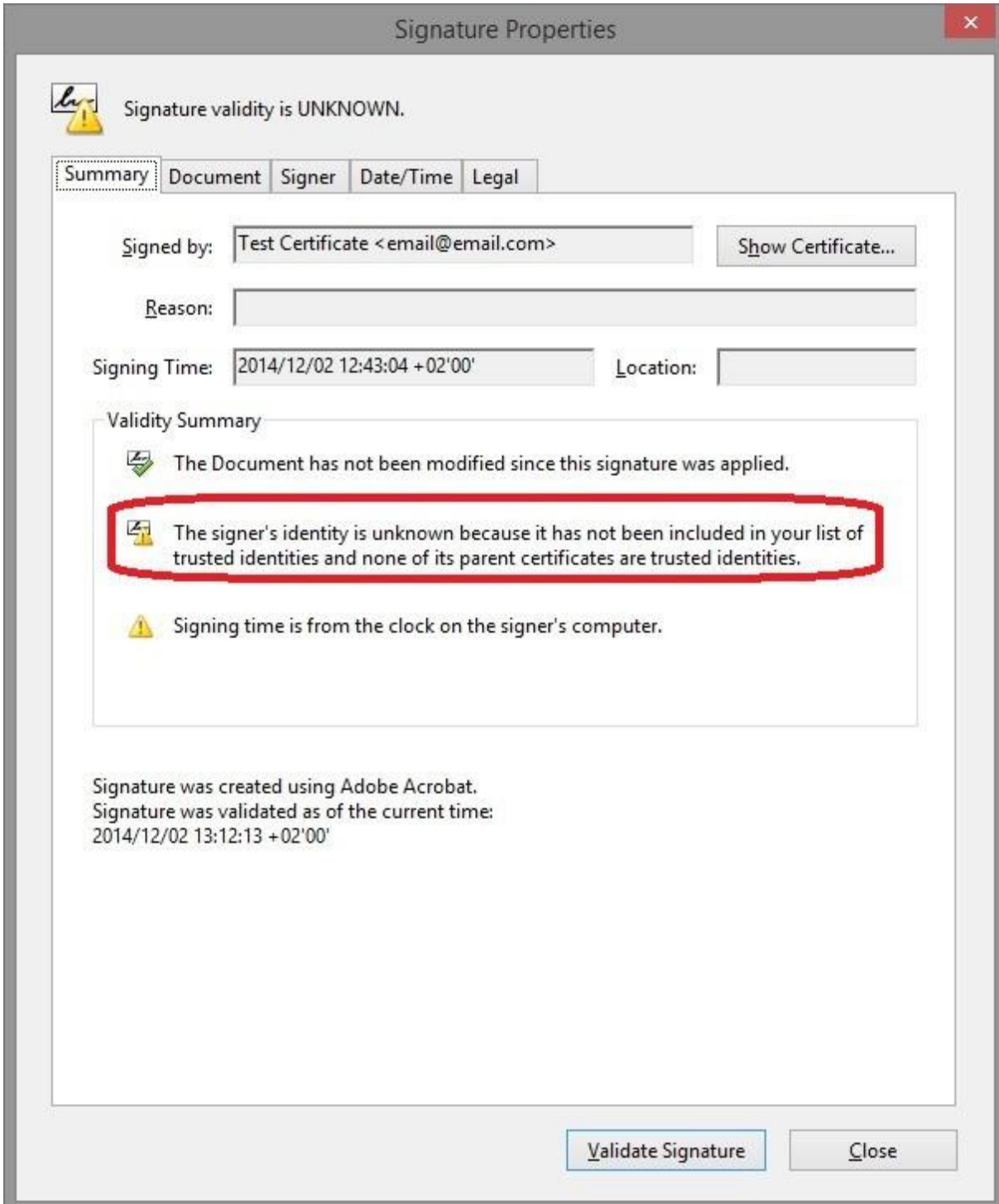
The digital signature is not trusted

- **Click on Signer tab**

Signature is not trusted

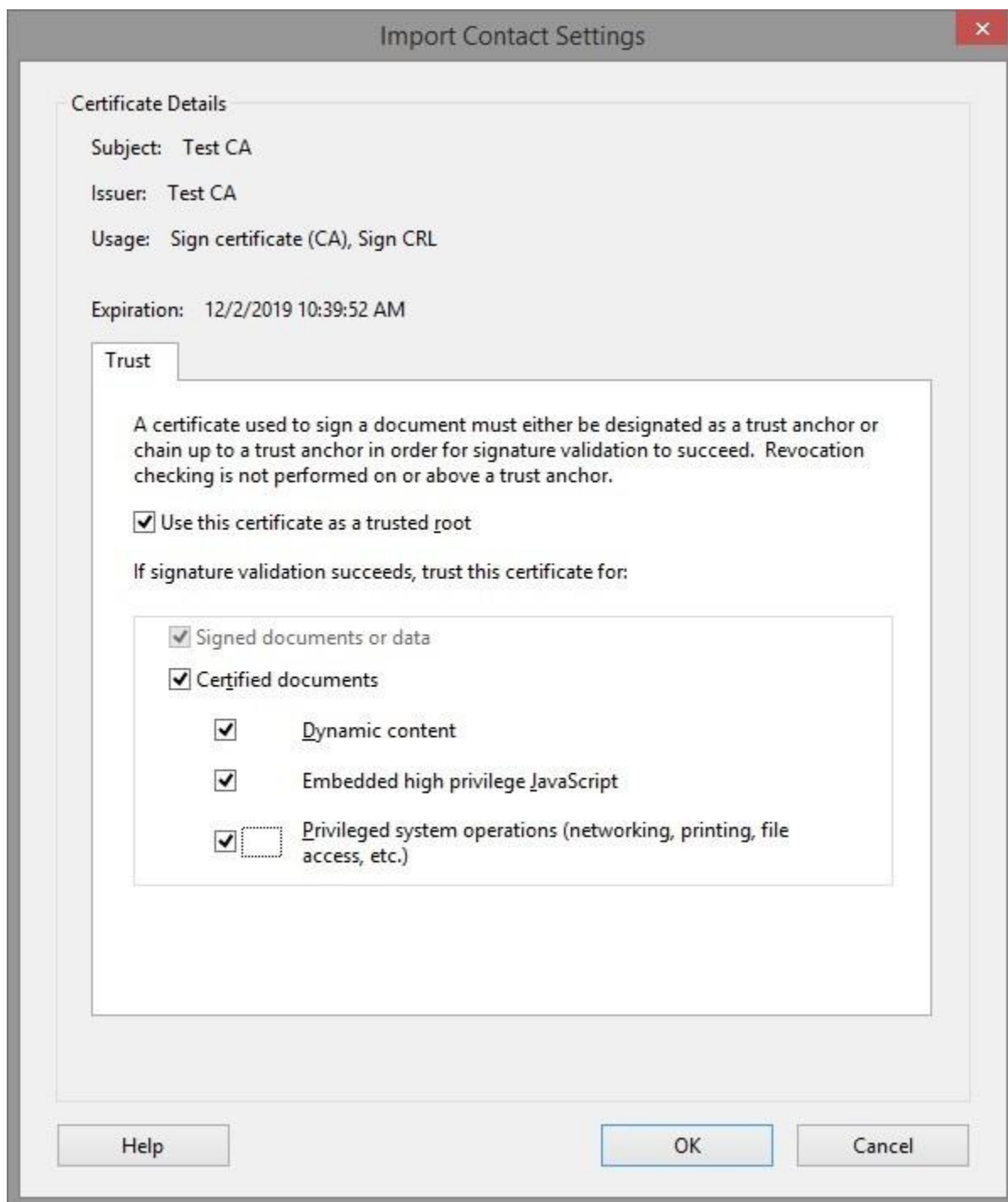To manually add the Root Certificate on the Adobe Trusted Identities, open the signature properties and click *Show Certificate and select Trust tab*.

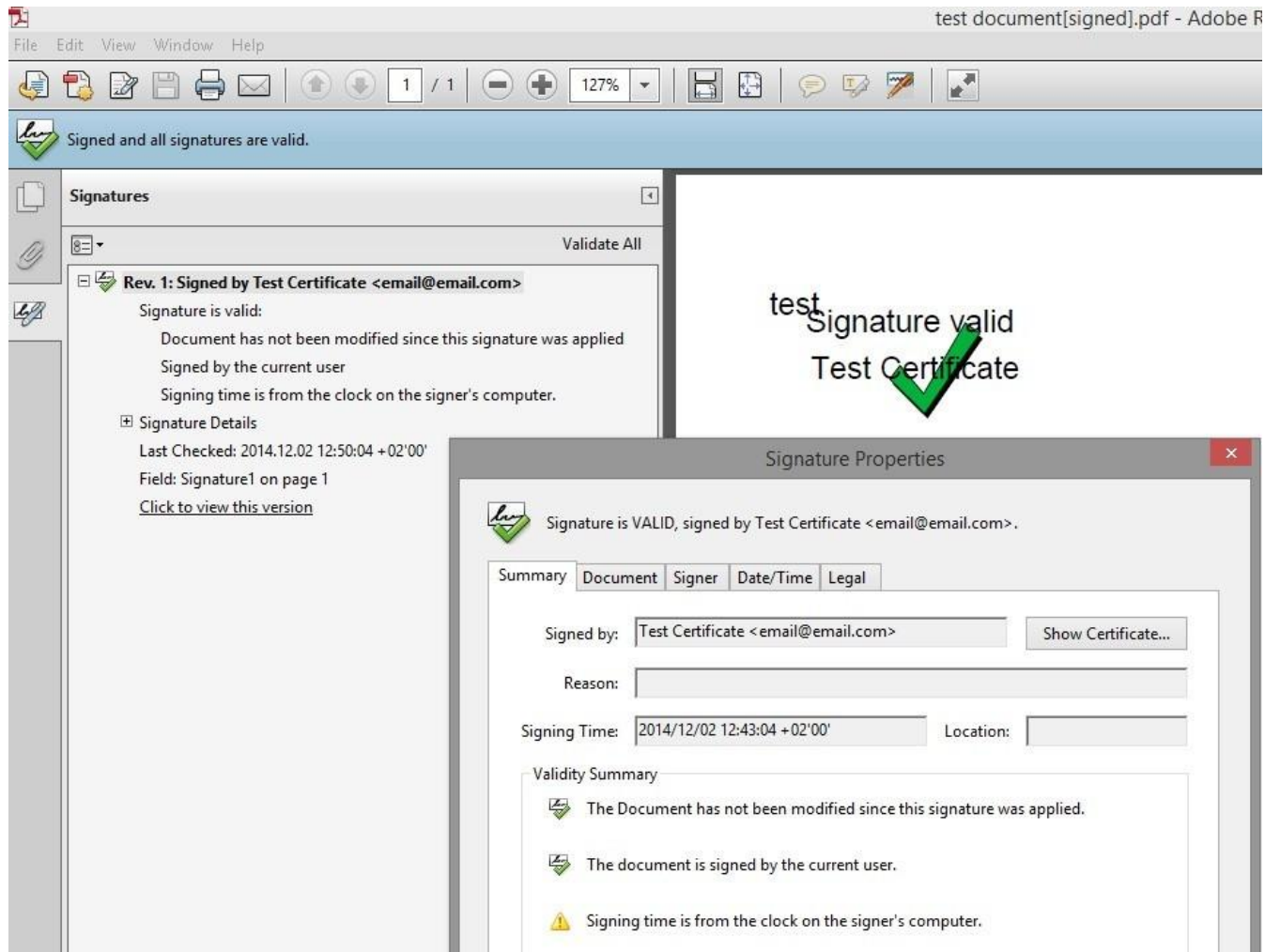**Be sure that you have selected the topmost Root Certificate.**
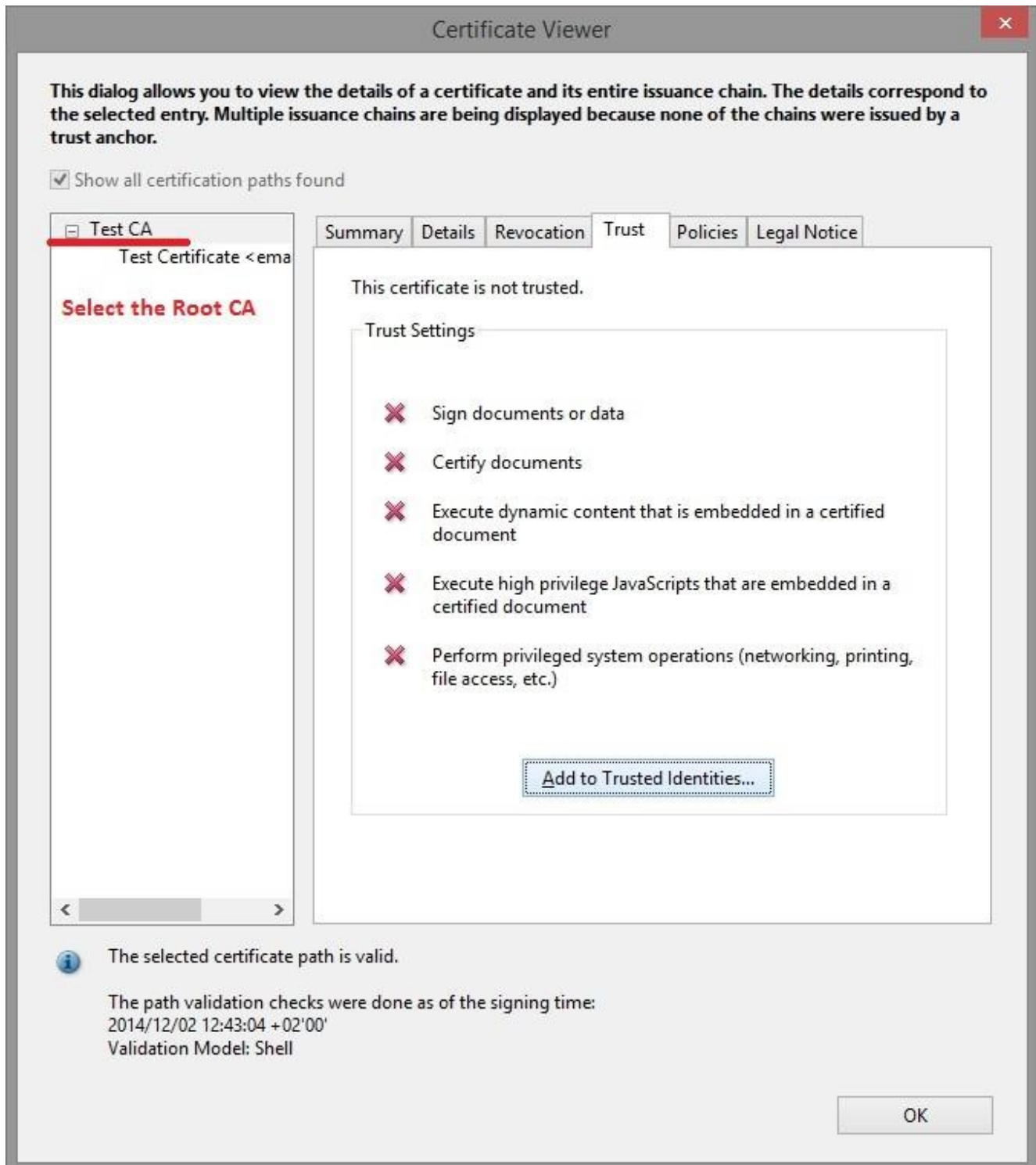
Press *Add to Trusted Identities tab* and be sure you have **checked all checkboxes**, as

Trust a CA certificate

After all dialog boxes are closed and the document is re-opened, **the signature is considered Valid**

Valid digital signature

The Root Certificate is now Trusted and all signatures generated with this Root Certificate will be also trusted.

After this settings are saved, the document is considered valid by Adobe.