Add the Root Certificate on Adobe Trusted Identities

Some of the Root CA's are included by default in Windows Certificate Store (Trusted Root Certification Authorities) and only a few are included in Adobe Trusted Identities.

Because the Root CA of the signing certificate is not included on Adobe Trusted Identities, the signature is considered "not trusted" (but NOT invalid).
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.

---

![Certificate Viewer window](image-url)  
*Certificate Viewer*

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry. Multiple issuance chains are being displayed because none of the chains were issued by a trust anchor.

- **Test CA**
  - Test Certificate < email

### Select the Root CA

#### Trust Settings

- **Cross** - Sign documents or data
- **Cross** - Certify documents
- **Cross** - Execute dynamic content that is embedded in a certified document
- **Cross** - Execute high privilege JavaScripts that are embedded in a certified document
- **Cross** - Perform privileged system operations (networking, printing, file access, etc.)

[Add to Trusted Identities...]

---

The selected certificate path is valid.

The path validation checks were done as of the signing time:

2014/12/02 12:43:04 +02'00'

Validation Model: Shell

---

*Trust a CA certificate*
Press Add to Trusted Identities tab and be sure you have checked all checkboxes, as below.

Trust a CA certificate
After all dialog boxes are closed and the document is re-opened, the signature is considered Valid.
The Root Certificate is now Trusted and all signatures generated with this Root Certificate will be also trusted.