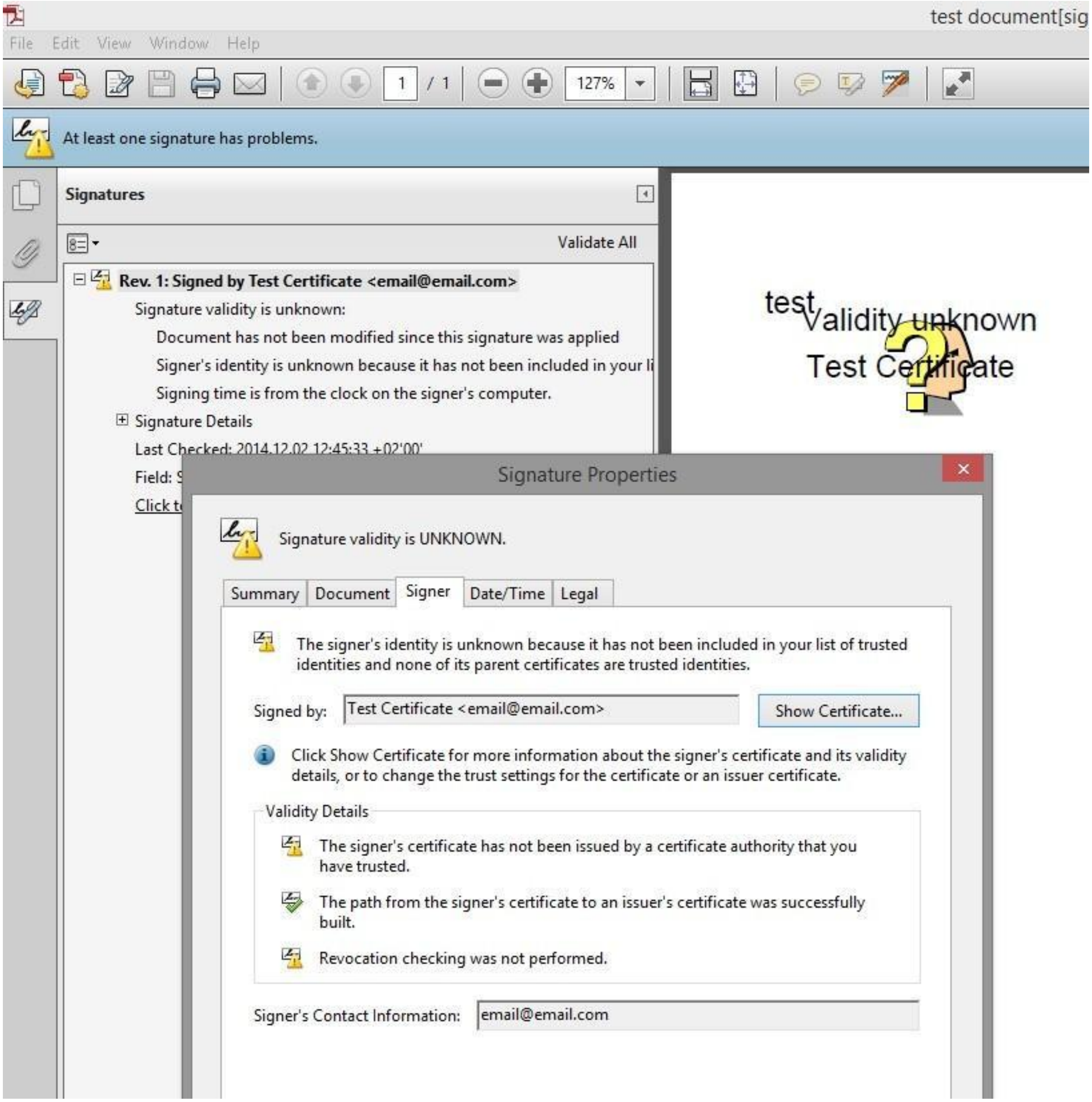
Add the Root Certificate on Adobe Trusted Identities

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).



At least one signature has problems.

Rev. 1: Signed by Test Certificate <email@email.com>

Signature validity is unknown:

Document has not been modified since this signature was applied

Signer's identity is unknown because it has not been included in your li

Signing time is from the clock on the signer's computer.

Signature Details

Last Checked: 2014.12.02 12:45:33 +02'00'

Field: S

Click t

Validity unknown

Test Certificate

Signature validity is UNKNOWN.

The signer's identity is unknown because it has not been included in your list of trusted identities and none of its parent certificates are trusted identities.

Signed by: Test Certificate <email@email.com>

Click Show Certificate for more information about the signer's certificate and its validity details, or to change the trust settings for the certificate or an issuer certificate.

Validity Details

The signer's certificate has not been issued by a certificate authority that you have trusted.

The path from the signer's certificate to an issuer's certificate was successfully built.

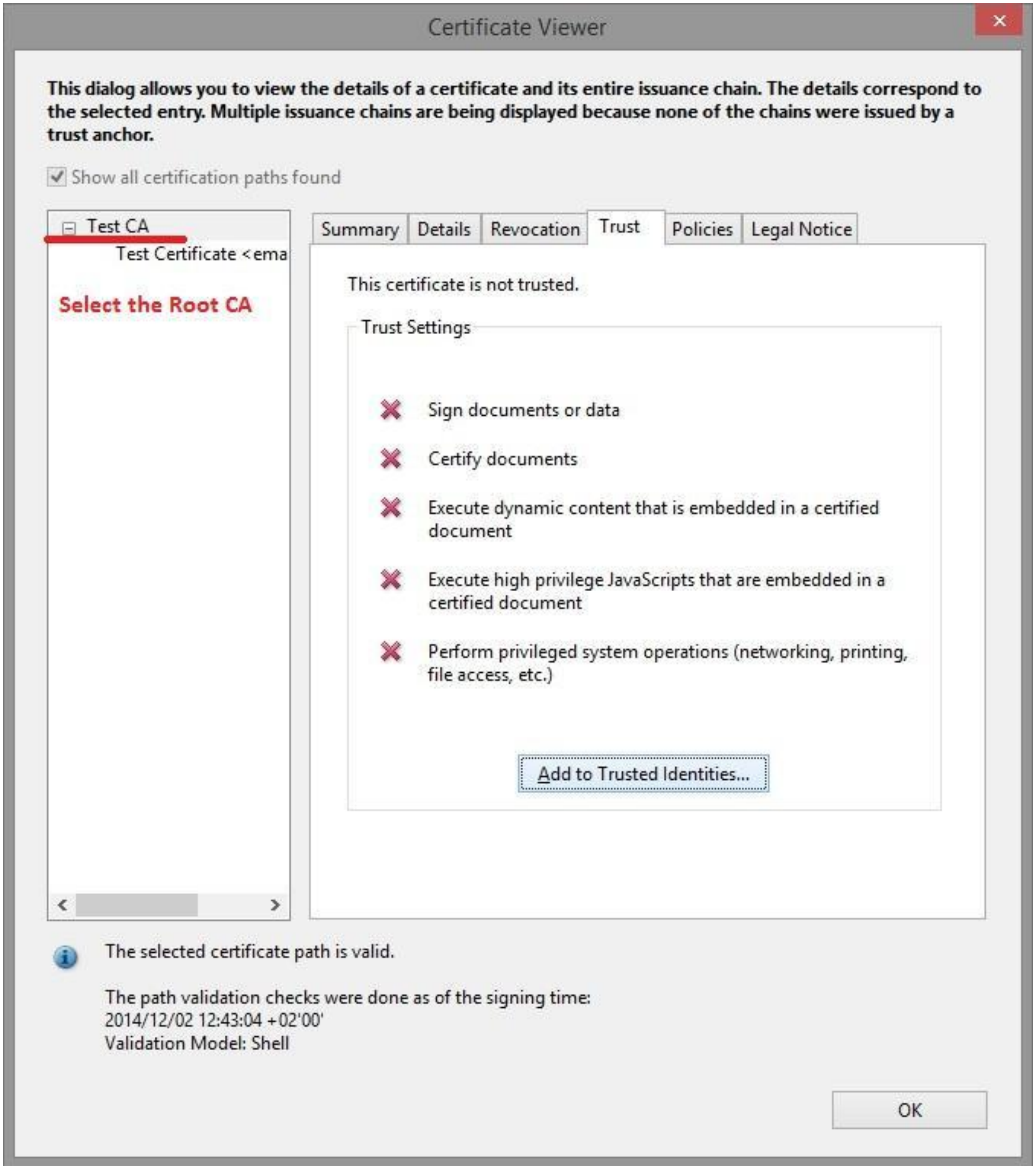
Revocation checking was not performed.

Signer's Contact Information: email@email.com

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.



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.

☑ Show all certification paths found

⊟ Test CA
Test Certificate <ema

Select the Root CA

This certificate is not trusted.

Trust Settings

☒ Sign documents or data

☒ Certify documents

☒ Execute dynamic content that is embedded in a certified document

☒ Execute high privilege JavaScripts that are embedded in a certified document

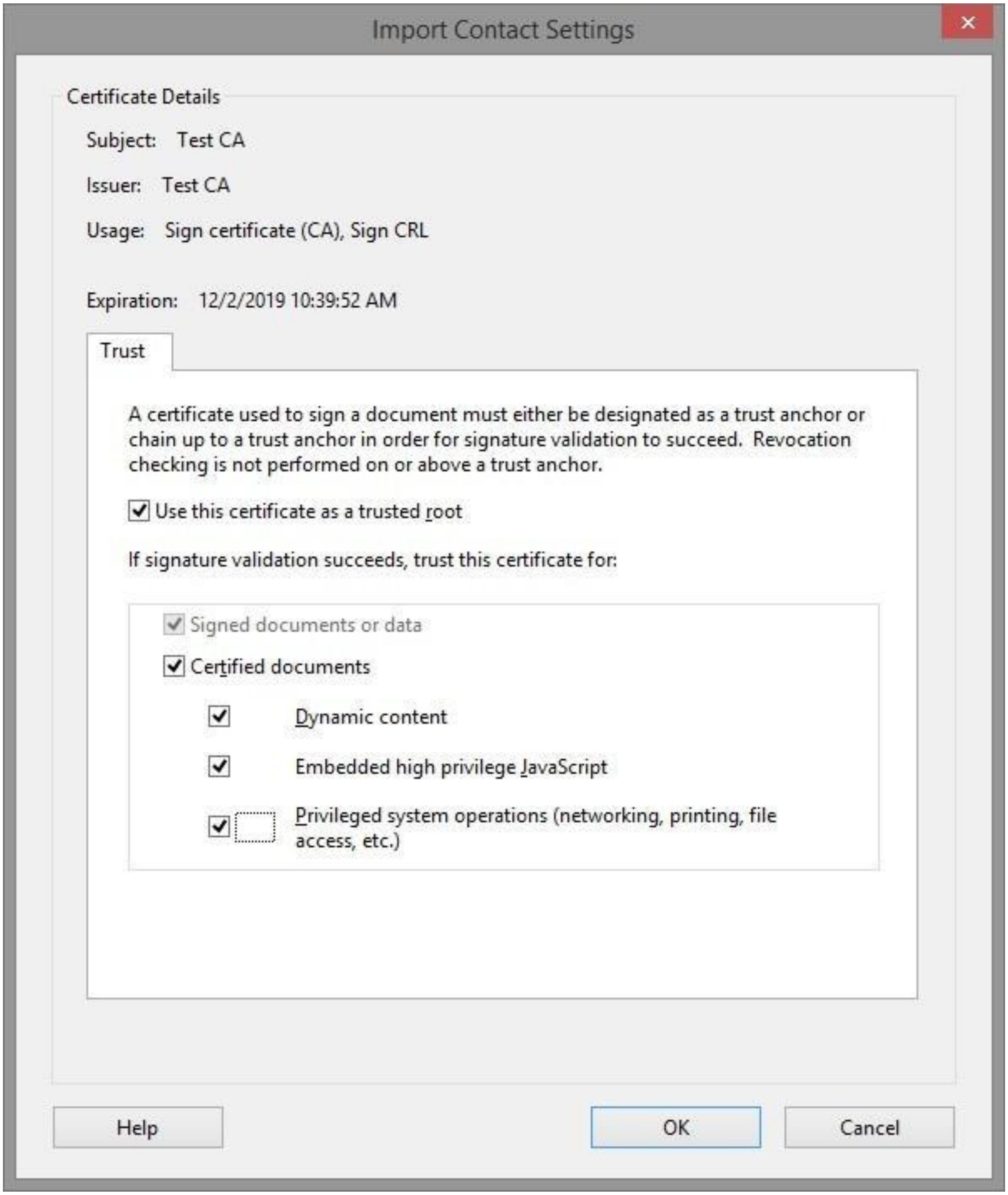
☒ Perform privileged system operations (networking, printing, file access, etc.)

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.



Import Contact Settings

Certificate Details

Subject: Test CA

Issuer: Test CA

Usage: Sign certificate (CA), Sign CRL

Expiration: 12/2/2019 10:39:52 AM

Trust

A certificate used to sign a document must either be designated as a trust anchor or chain up to a trust anchor in order for signature validation to succeed. Revocation checking is not performed on or above a trust anchor.

☑ Use this certificate as a trusted root

If signature validation succeeds, trust this certificate for:

☑ Signed documents or data

☑ Certified documents

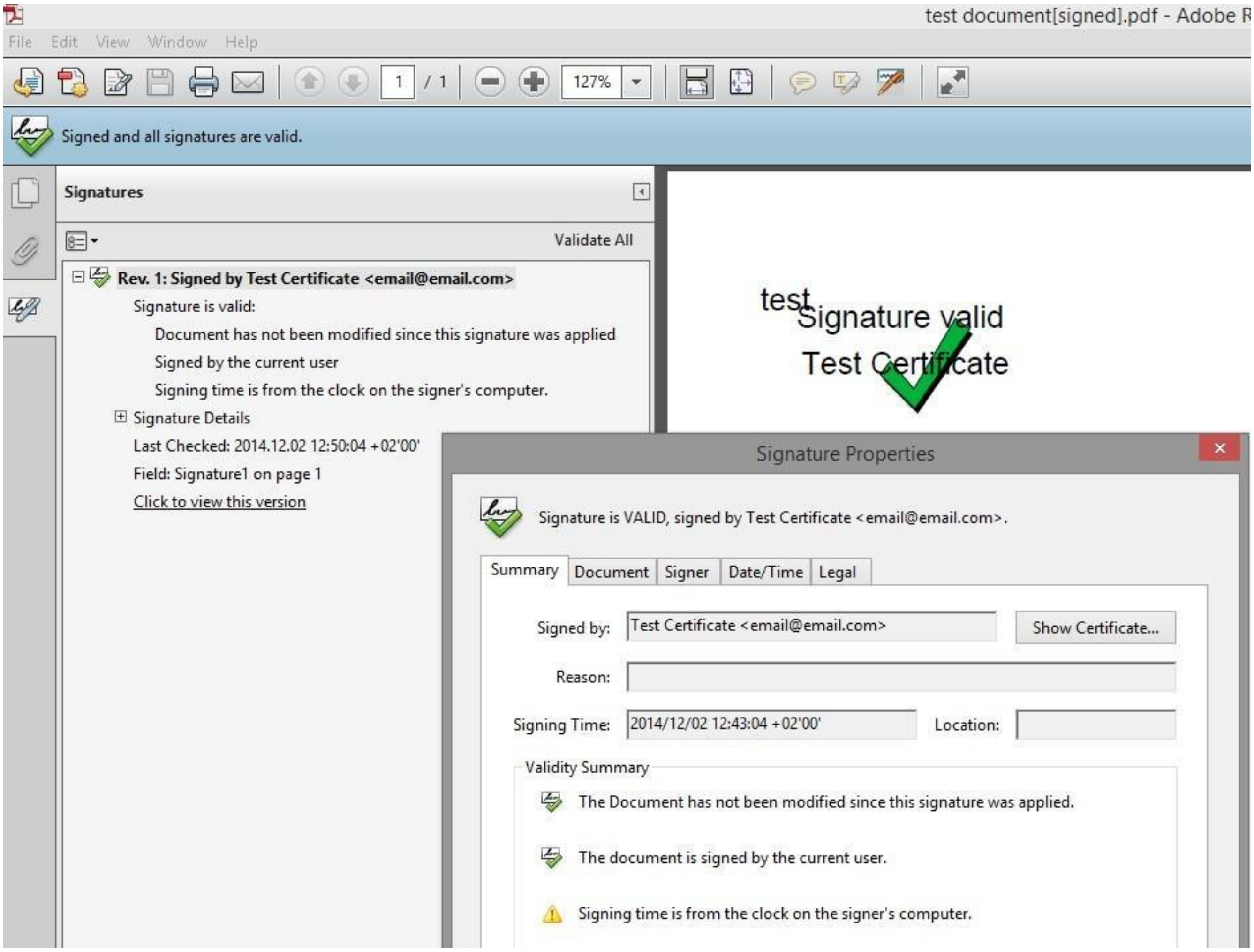
☑ Dynamic content

☑ Embedded high privilege JavaScript

☑ Privileged system operations (networking, printing, file access, etc.)

Trust a CA certificate

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



Signed and all signatures are valid.

Rev. 1: Signed by Test Certificate <email@email.com>

Signature is valid:

Document has not been modified since this signature was applied

Signed by the current user

Signing time is from the clock on the signer's computer.

⊞ Signature Details

Last Checked: 2014.12.02 12:50:04 +02'00'

Field: Signature1 on page 1

Click to view this version

Signature is VALID, signed by Test Certificate <email@email.com>.

Signed by: Test Certificate <email@email.com>

Reason:

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

Location:

Validity Summary

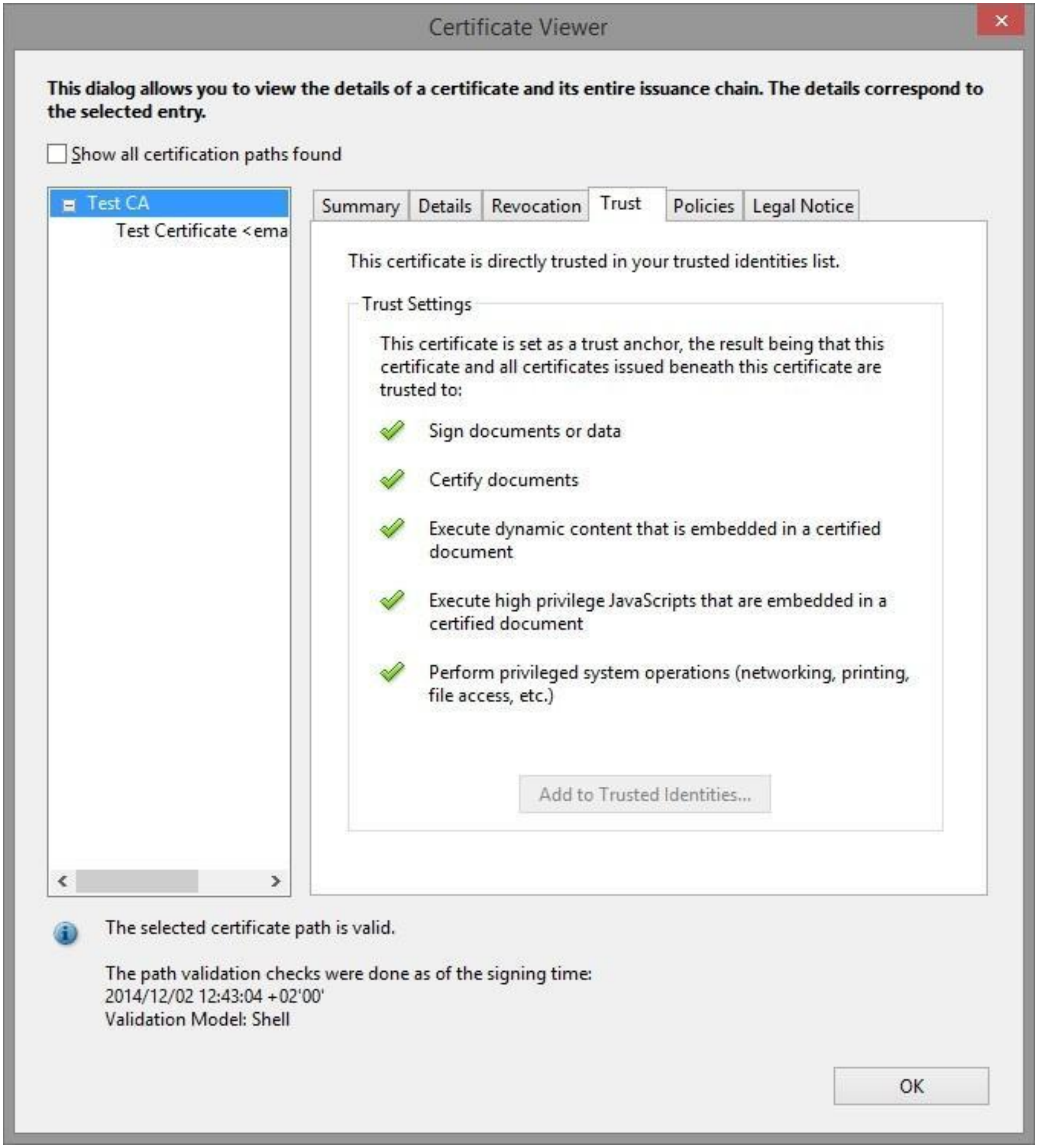
The Document has not been modified since this signature was applied.

The document is signed by the current user.

⚠ Signing time is from the clock on the signer's computer.

Valid digital signature

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



This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

□ Show all certification paths found

This certificate is directly trusted in your trusted identities list.

Trust Settings

This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to:

✓ Sign documents or data

✓ Certify documents

✓ Execute dynamic content that is embedded in a certified document

✓ Execute high privilege JavaScripts that are embedded in a certified document

✓ Perform privileged system operations (networking, printing, file access, etc.)

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

Trusted Root Certificate