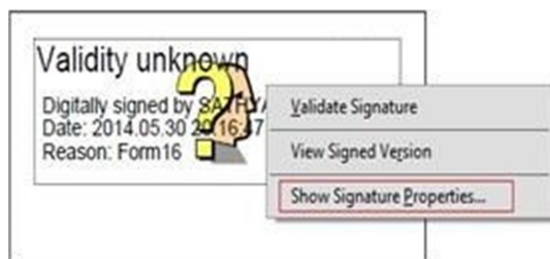


## STEPS TO VALIDATE THE DIGITAL SIGNATURE

### Step by Step Guide to Validate the Digitally Signed PDF Files

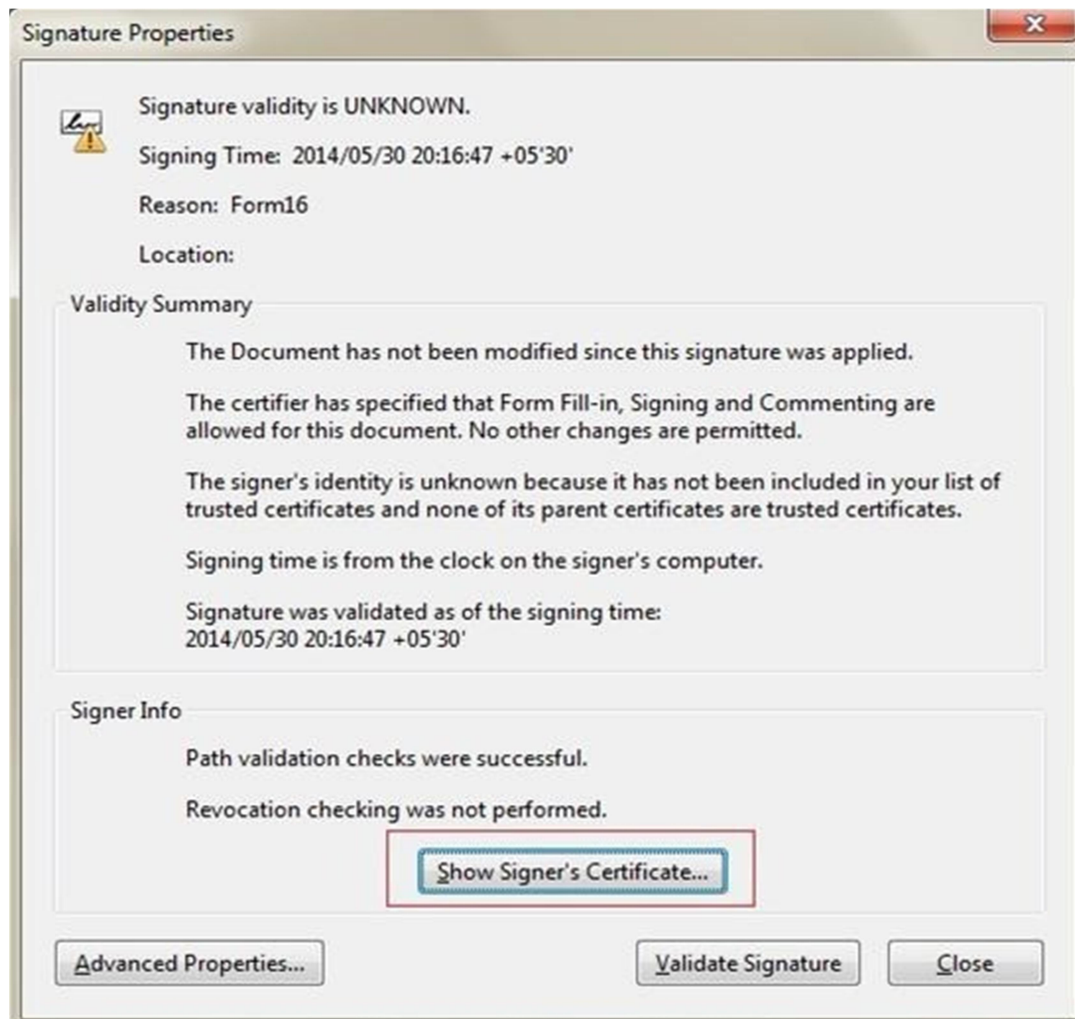
#### Step 1:

Right click the mouse and click "Show Signature Properties".



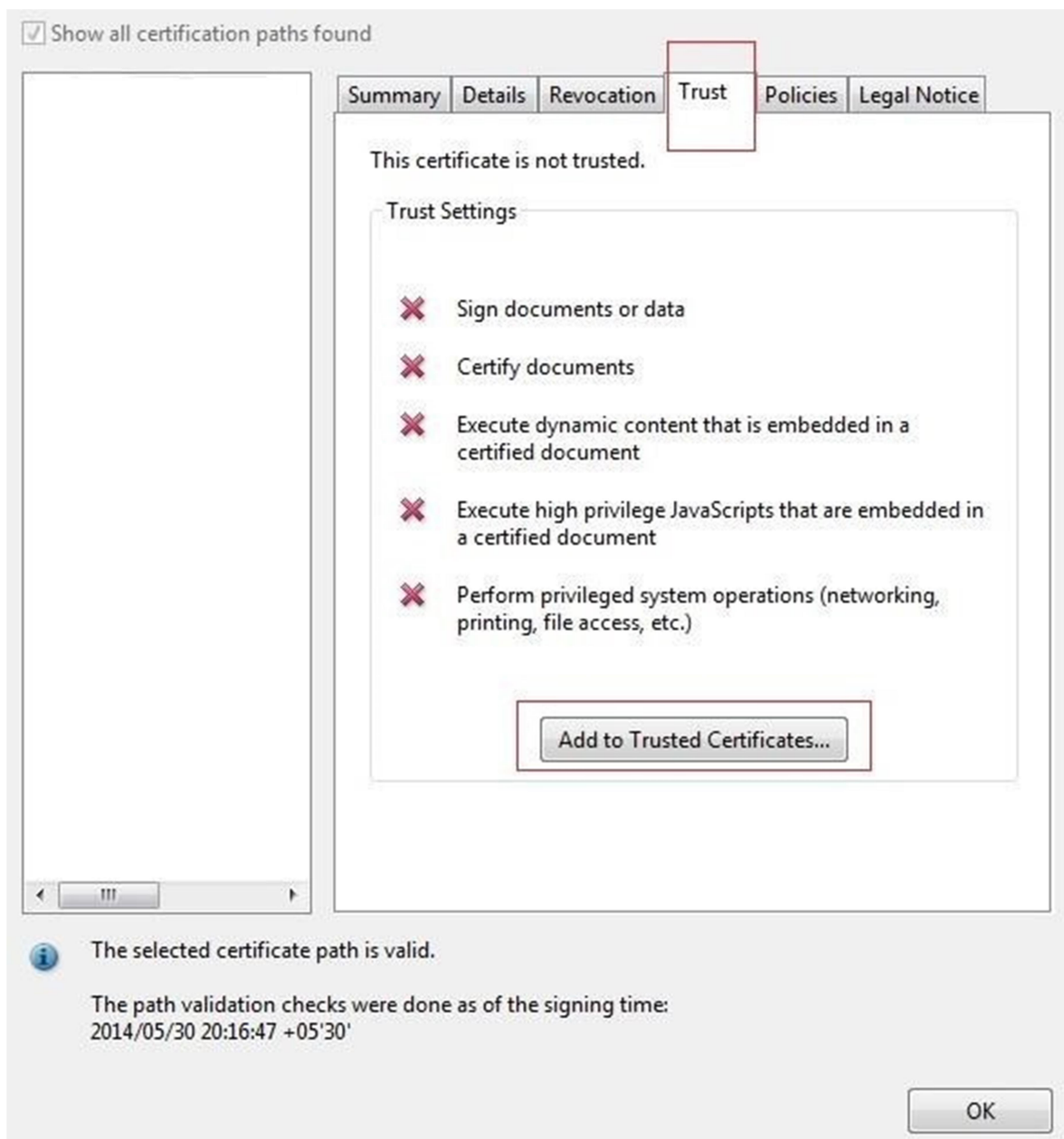
Step 2:

Click on "Show Signer's certificate".



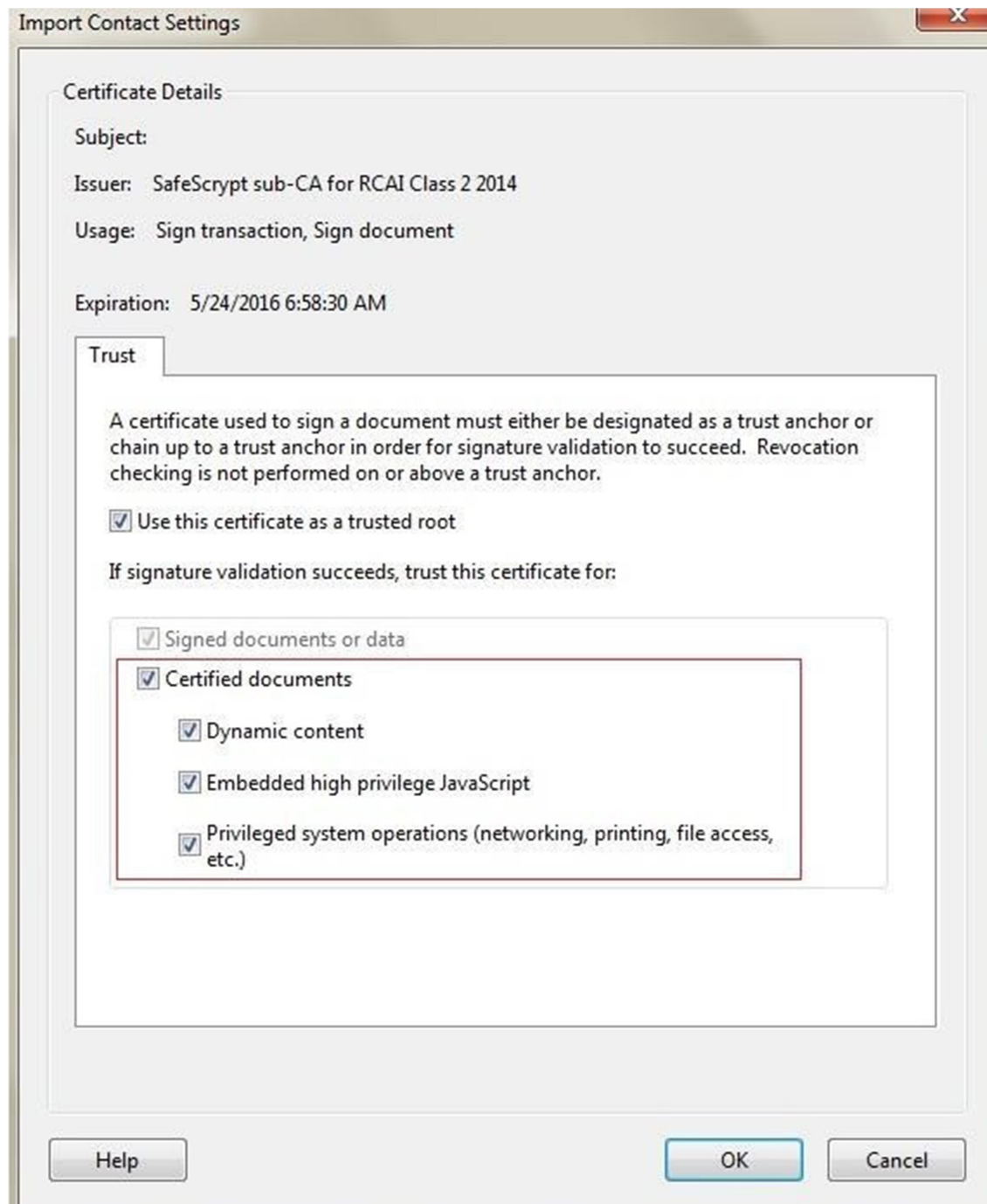
### Step 3:

- Go to “Trust” tab .
- After that click “Add to Trusted Certificates”.



Step 4:

Select all the check boxes as below and click "OK" button to proceed further.



The image shows a Windows-style dialog box titled "Import Contact Settings". It has a standard title bar with a close button (X). The dialog is divided into two main sections: "Certificate Details" and "Trust".

**Certificate Details**

Subject:

Issuer: SafeScript sub-CA for RCAI Class 2 2014

Usage: Sign transaction, Sign document

Expiration: 5/24/2016 6:58:30 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.)

At the bottom of the dialog, there are three buttons: "Help", "OK", and "Cancel".

Step 5:

Finally, click on "Validate Signature" button



Once the signature is validated, you will be able to see signatory's name and description of signature certificate below the Menu Bar.

.....-X-.....-