# Step 6
# How to Check the Validity of Digitally Signed Documents (For Document Recipients)

When you receive an electronic document that has a digital signature affixed, it is your responsibility to make sure that the signature on the document is a valid one.

**How to Trust LankaSign Root & Intermediate Certificates in Adobe Acrobat:**

This section is only a one time required setup.

1.  Download
    ✓ **LankaSign Root CA Certificate**
    ✓ **LankaSign Intermediate CA Certificate**
From the below link:

https://www.lankaclear.com/knowledge-center/lankasign/#downloads

2.  Extract both zip files and make a note of this folder path

3.  Open Adobe Acrobat
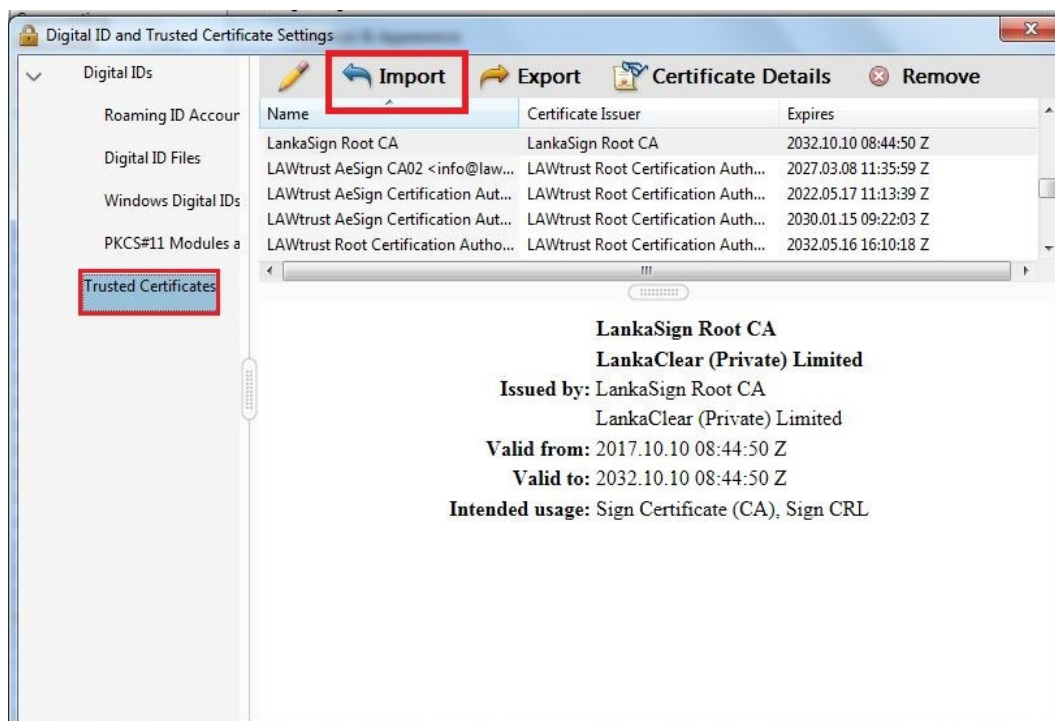
4.  Click on Edit→ Preferences
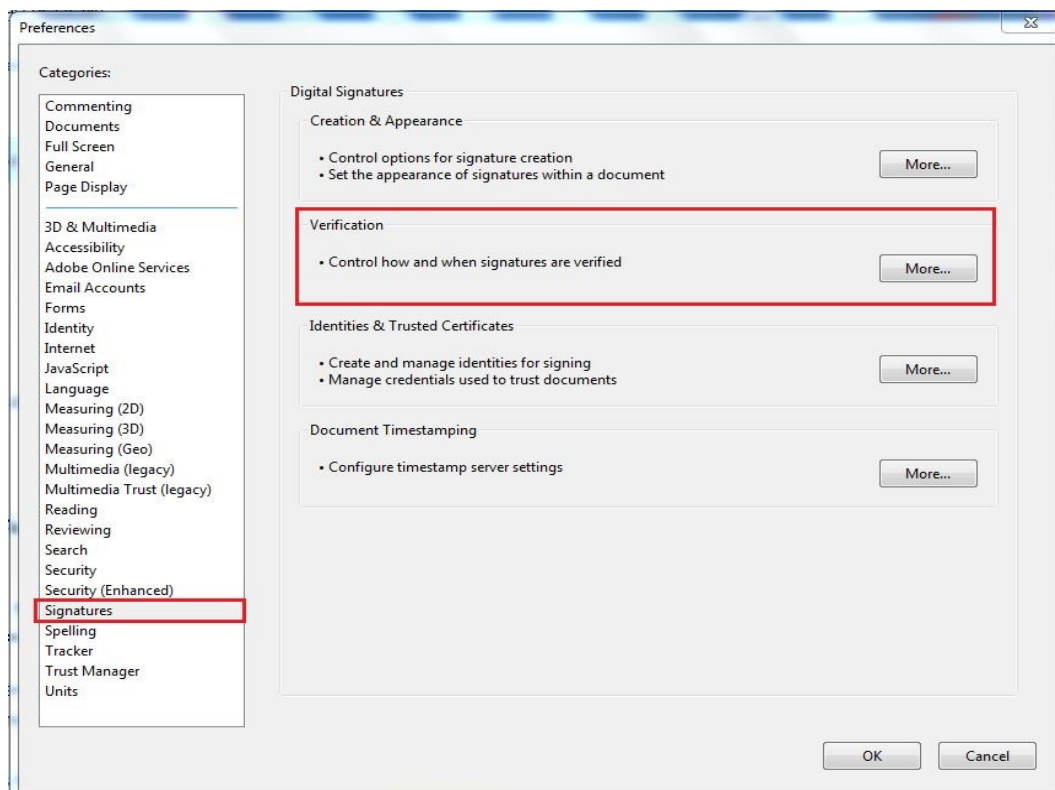
5. Click on Signatures → More button belonging to "**Verification**" section

6. Ensure "**Verify Signatures when document is opened**" tick box is checked and click on Ok.
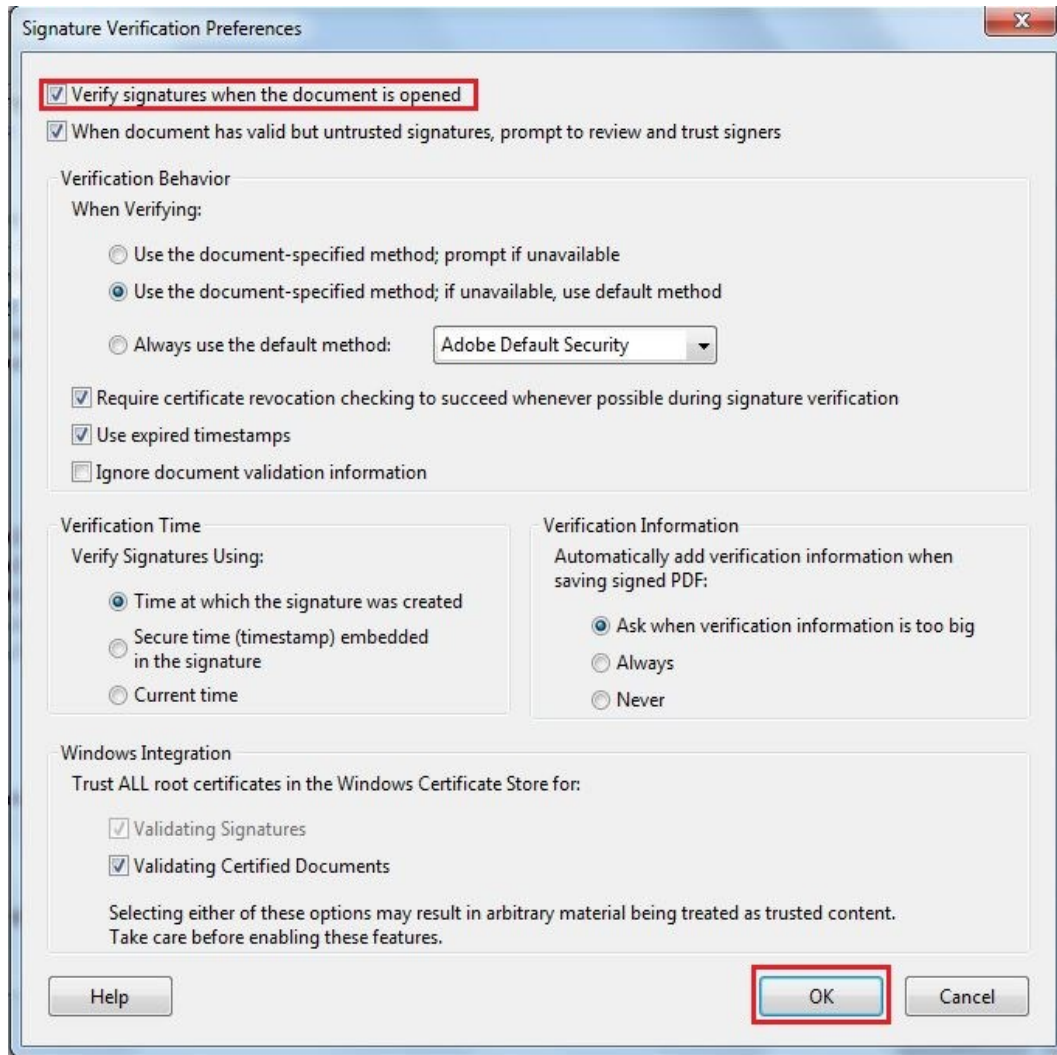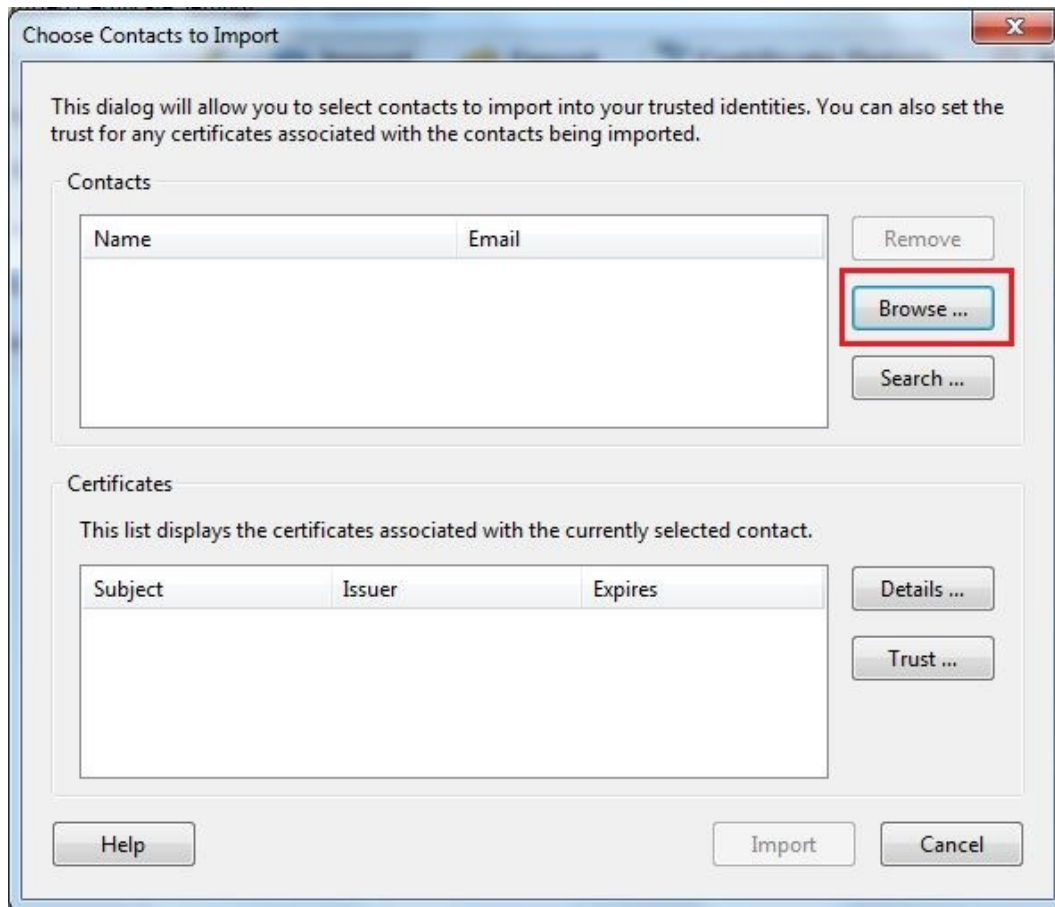
7. Now click on More button belonging to "**Identities and Trusted Certificates**" section
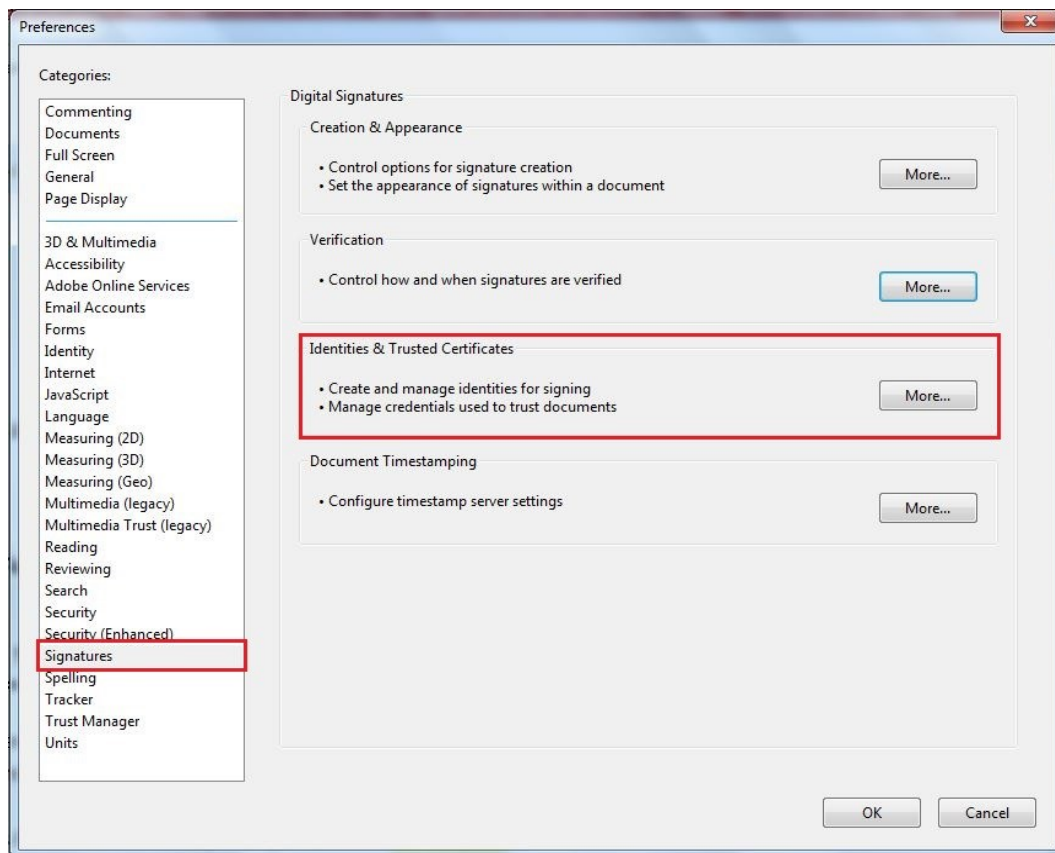


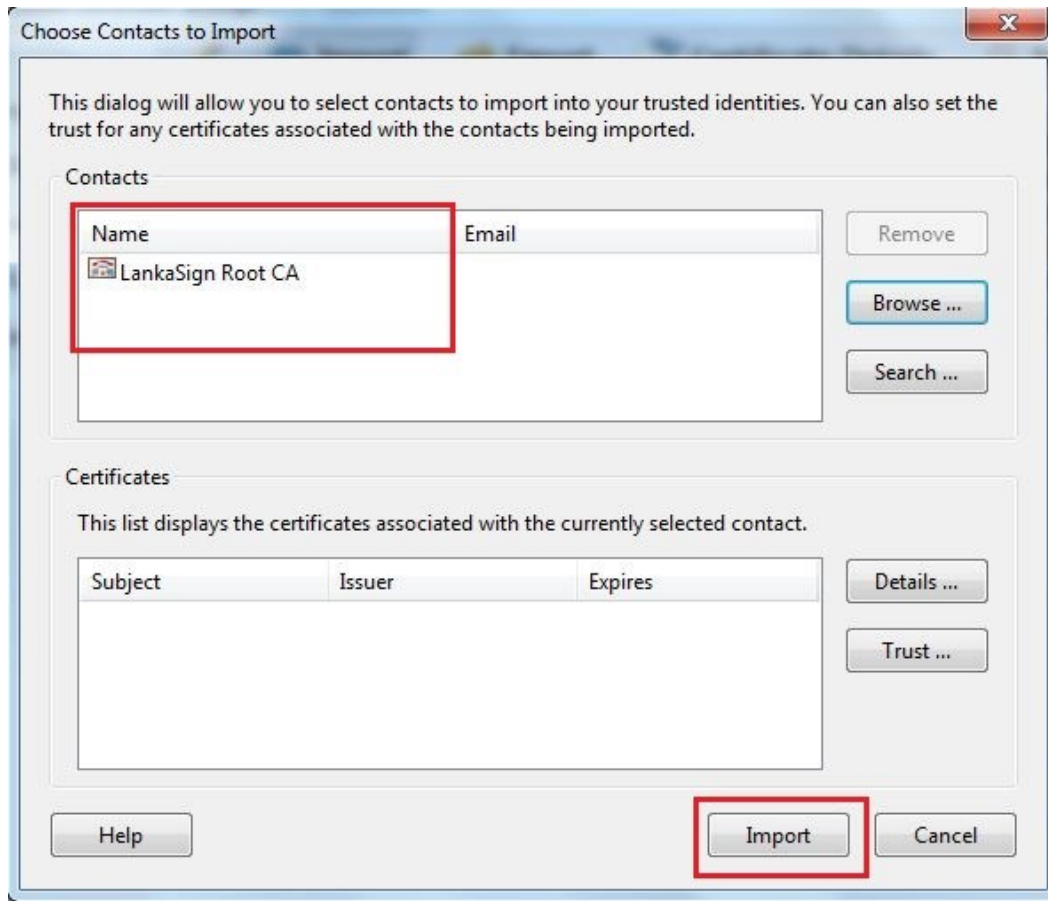8. Now click on "**Trusted Certificates**" and click on "**Import**"
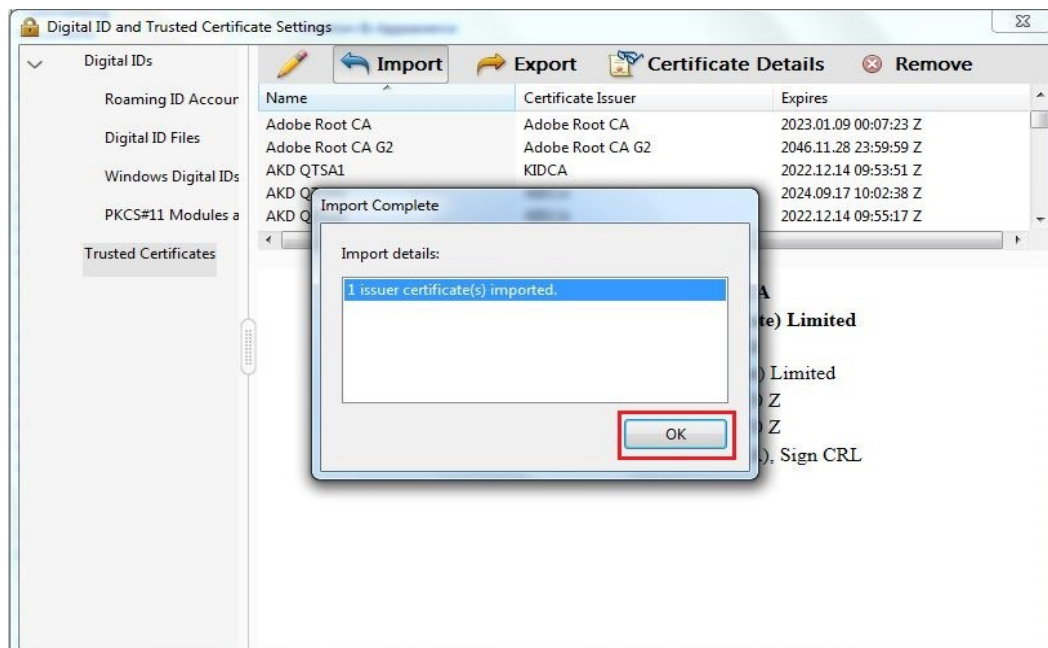
9. Now Click on **Browse**.



10. Now browse to the earlier noted folder path containing extracted **LankaSign Root CA** and **Intermediate CA** certificates.

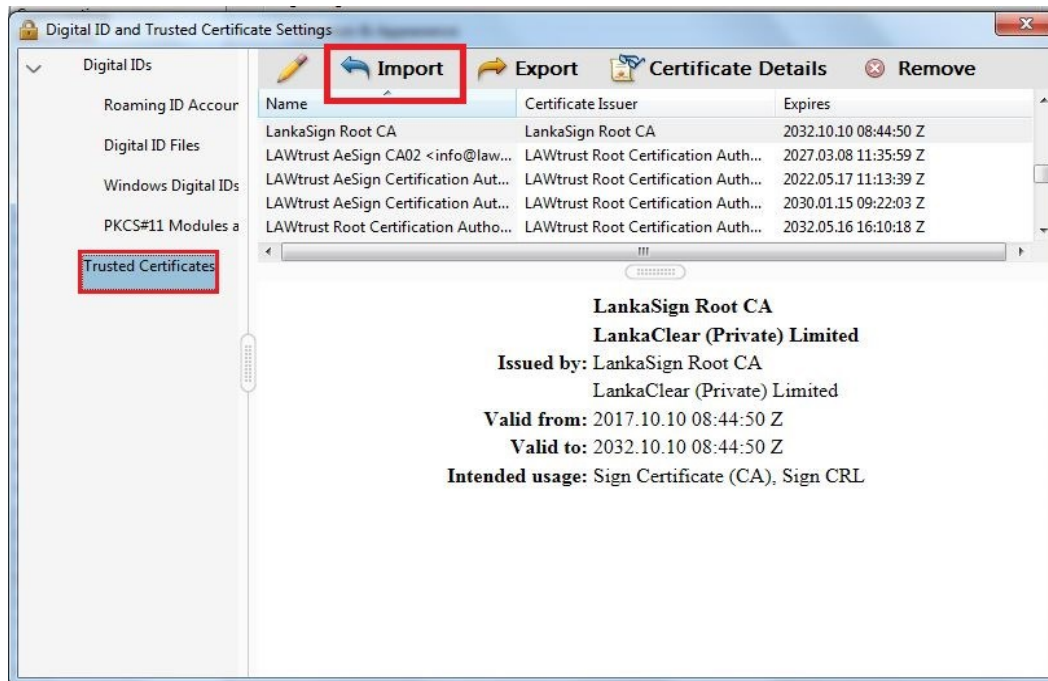11. Select **LankaSign Root CA Certificate** → Click on **Open**.

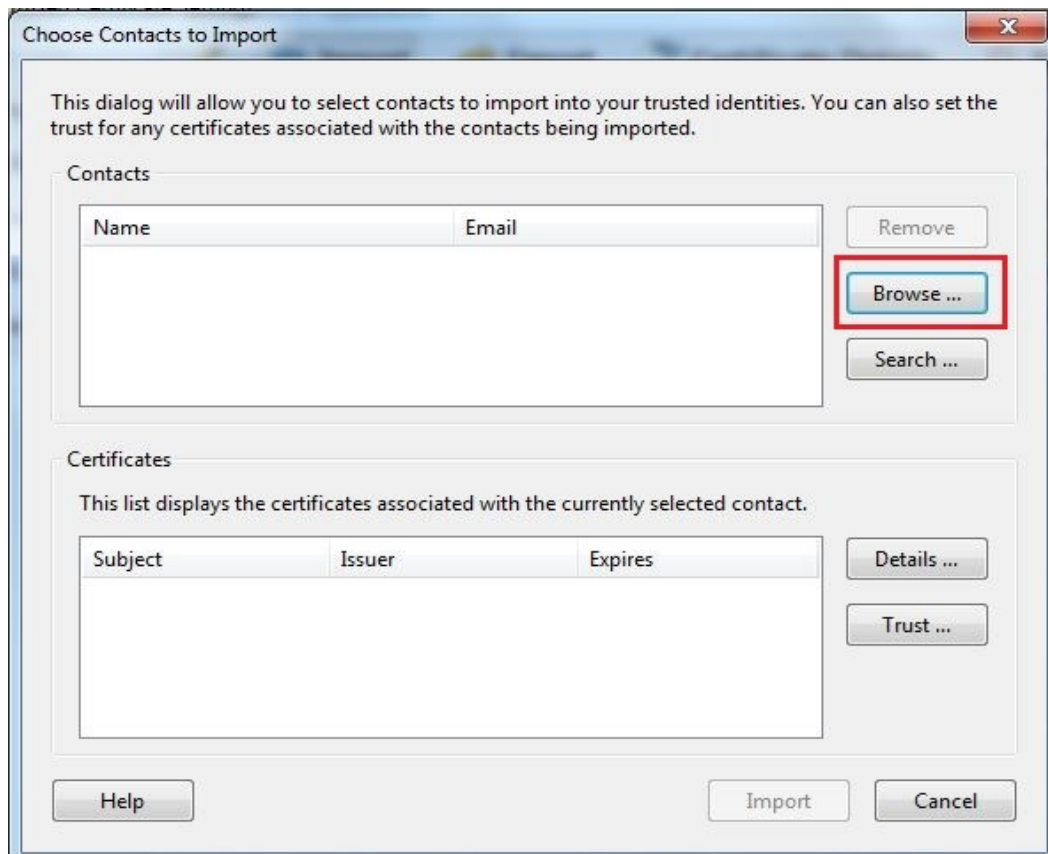12. Note the **LankaSign Root CA Certificate** → Click on **Import**.

13. Click **Ok** on Certificate **Import Complete message**. Now you have successfully imported LankaSign Root CA Certificate as a Trusted Certificate.
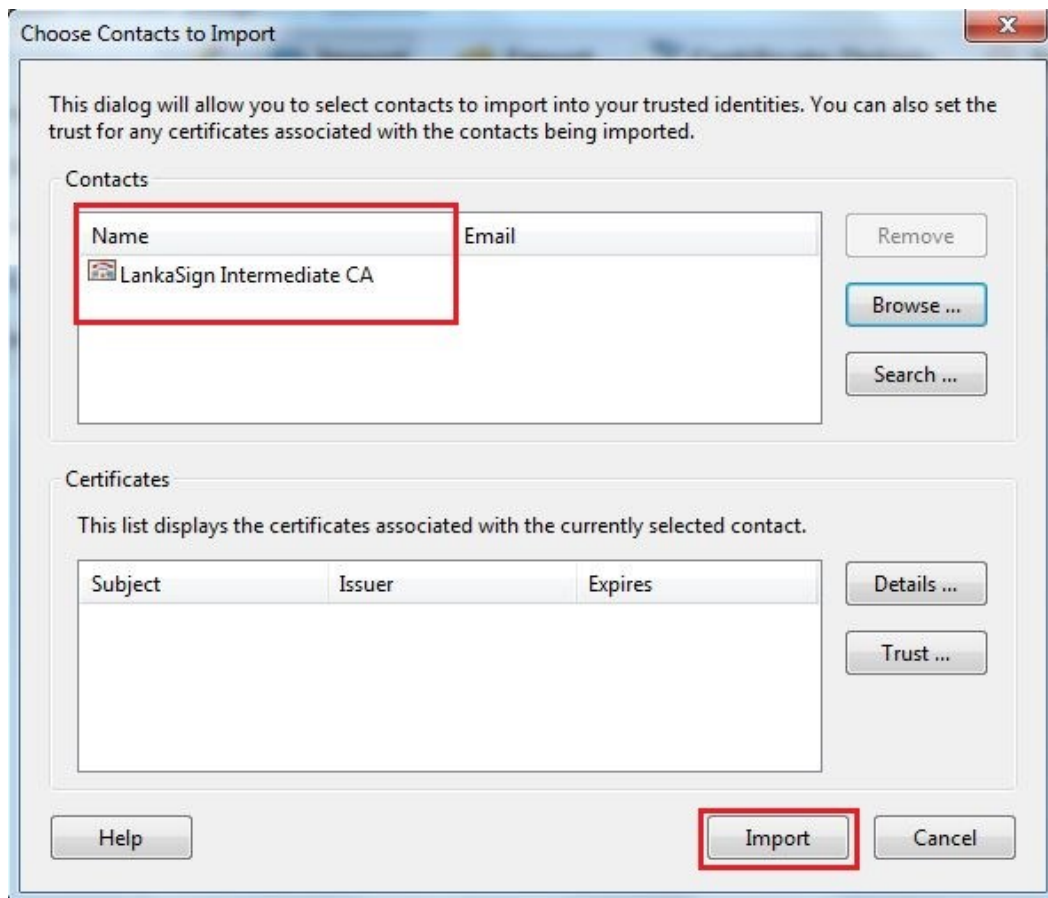
14. Now Click on **Import**



15. Now Click on **Browse**.

16. Now browse to the earlier noted folder path containing extracted LankaSign Root CA and Intermediate CA certificates.

17. Select **LankaSign Intermediate CA Certificate** → Click on **Open**.

18. Note the **LankaSign Intermediate CA Certificate** → Click on **Import**.
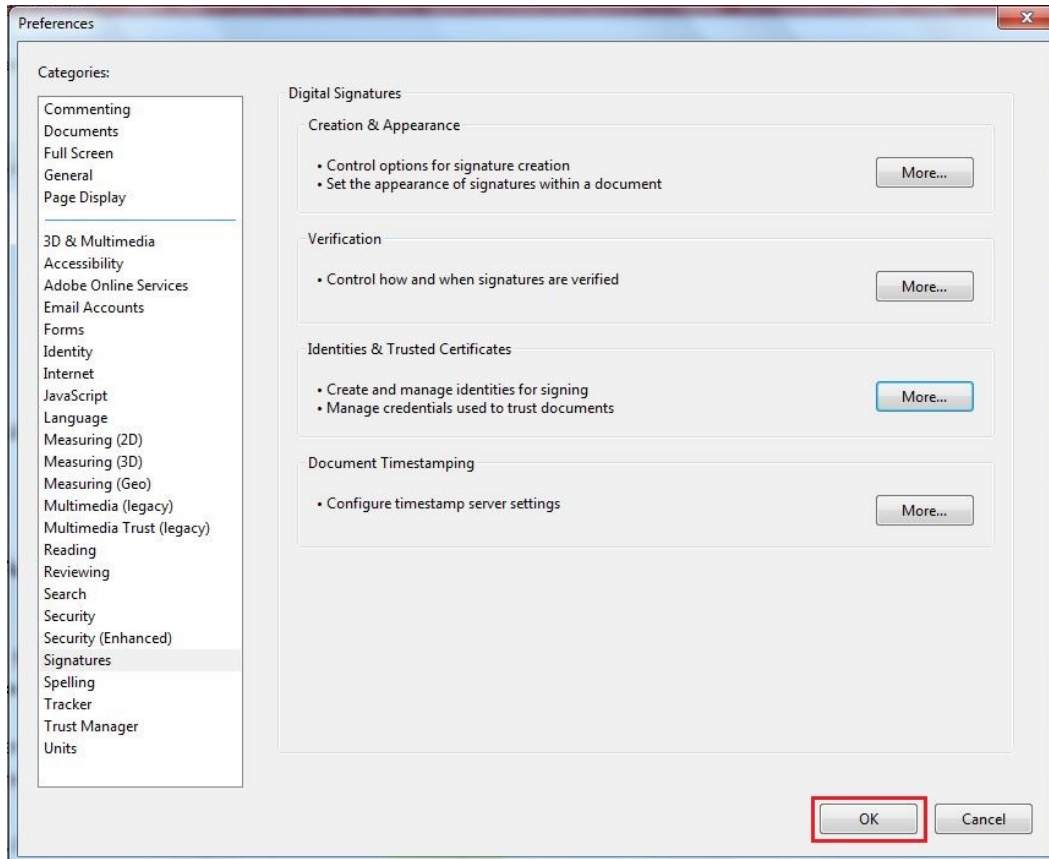
19. Click **Ok** on Certificate **Import Complete message**. Now you have successfully imported **LankaSign Intermediate CA Certificate** as a Trusted Certificate.
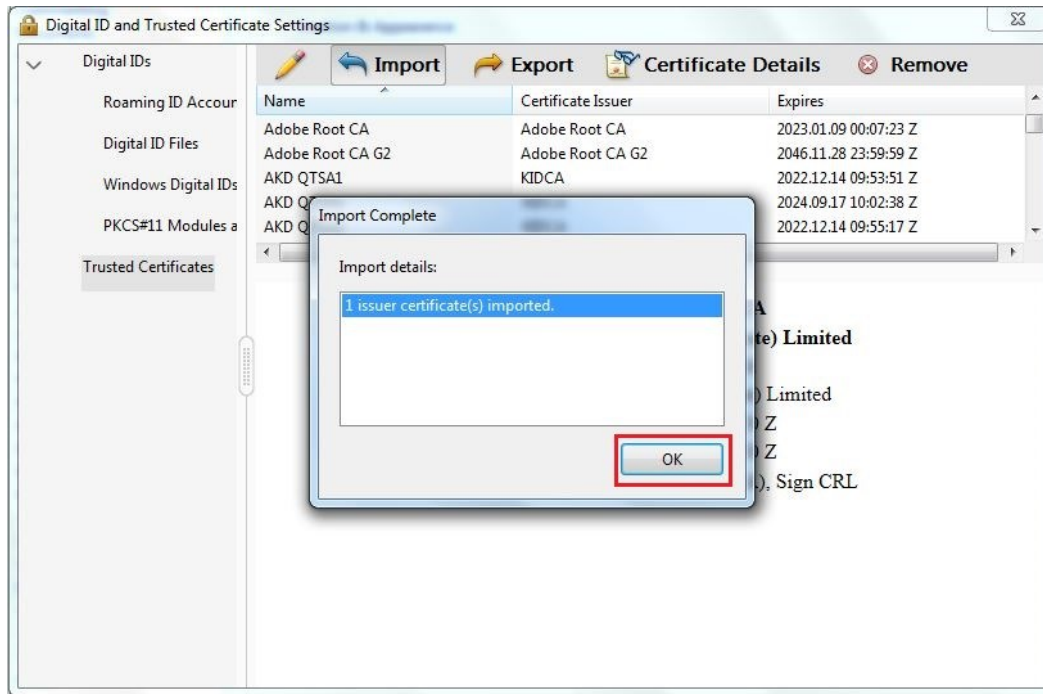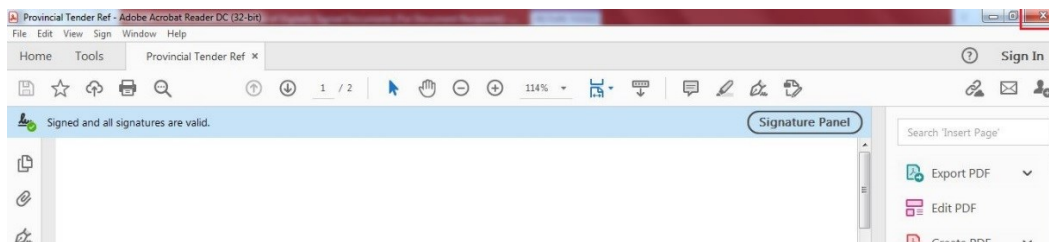


20. Make a note of LankaSign Root CA & Intermediate CA Certificates → Close the dialog box.
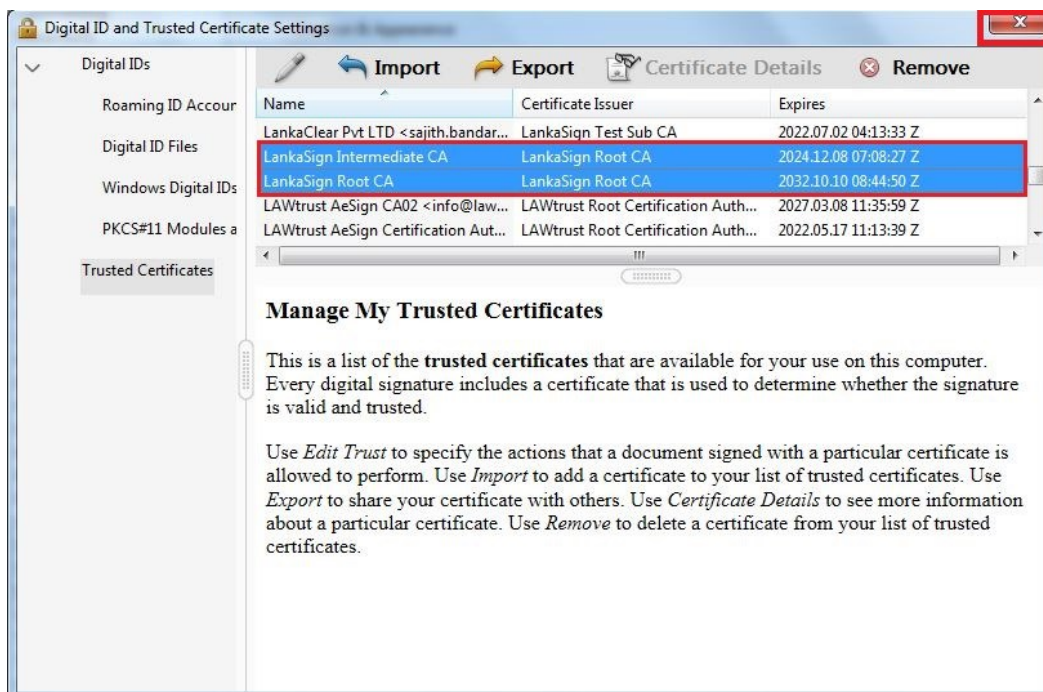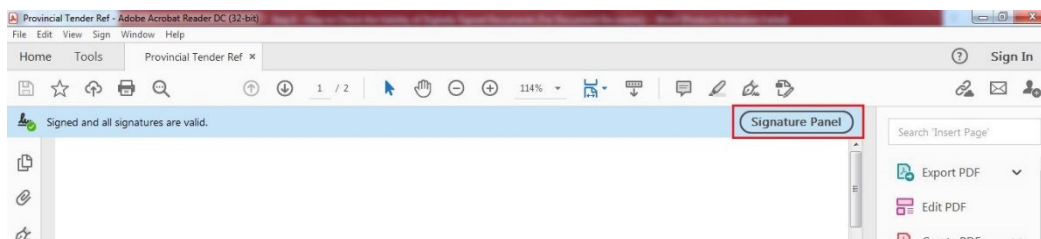
21. Click on Ok.
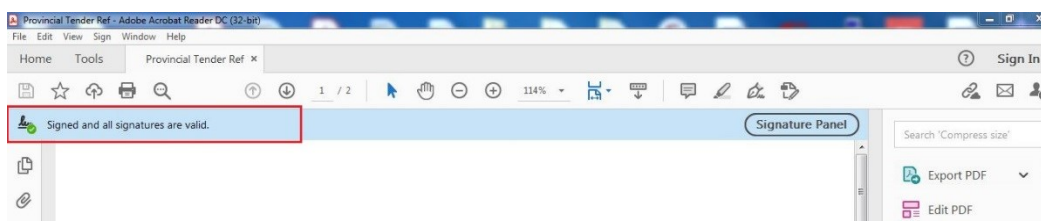


22. Now close the document.

**How to Check the Validity of Digitally Signed PDF Documents:**

1. Make sure your PC/laptop is connected to the internet

2. Open the **pdf document** → Click on **Signature Panel**.



3. Now check the **validity statuses**. The validation should happen automatically and the above status showing in the Signature panel's message ribbon.
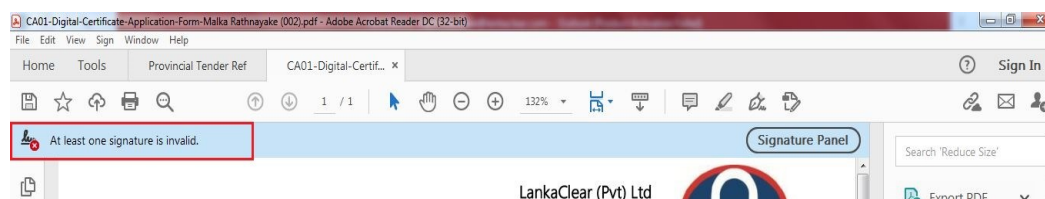
   ➢ **All signatures are valid**:



   The Document has been signed by valid certificate and not edited after signed.

   ➢ **Signed and all signatures are valid, but with unsigned changes after the last Signature**.
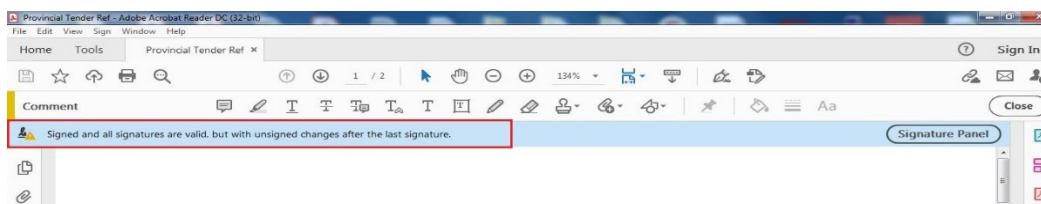


   The Document has been signed by a valid certificate but if the document edited after signed, the above status showing in the Signature panel's message ribbon.
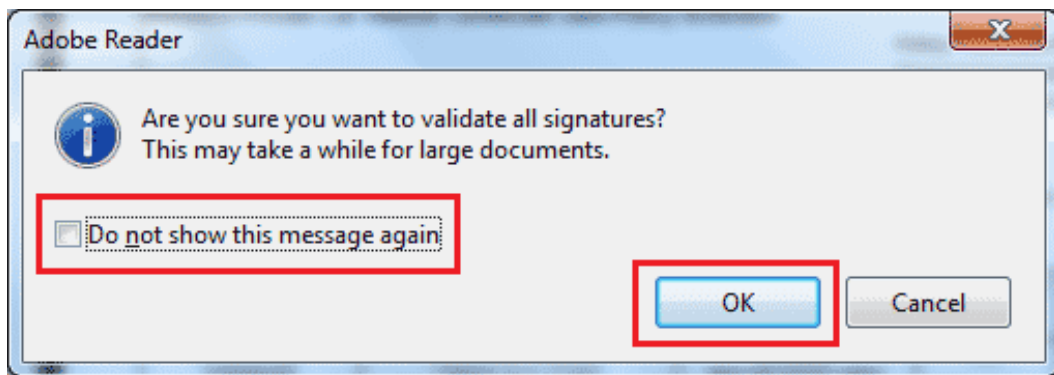
   ➢ **At least one signature is invalid.**



   The Document has been signed by an invalid or revoked certificate.
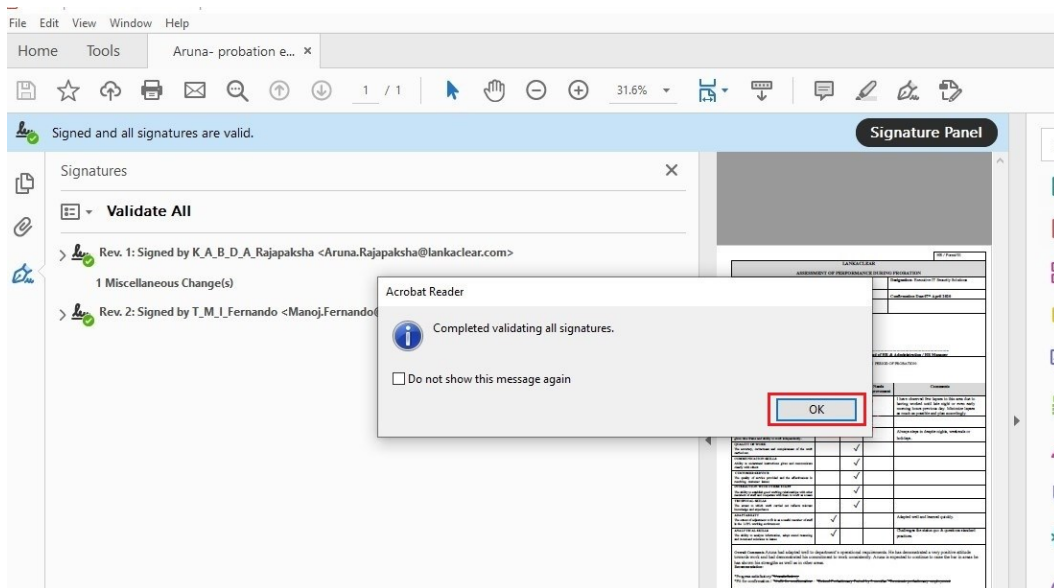
4. If automatic validation had not happened for any reason, it will indicate a problem. Click on Validate All. Skip steps 4 to 6 if all signatures are validated in already appears in green color.
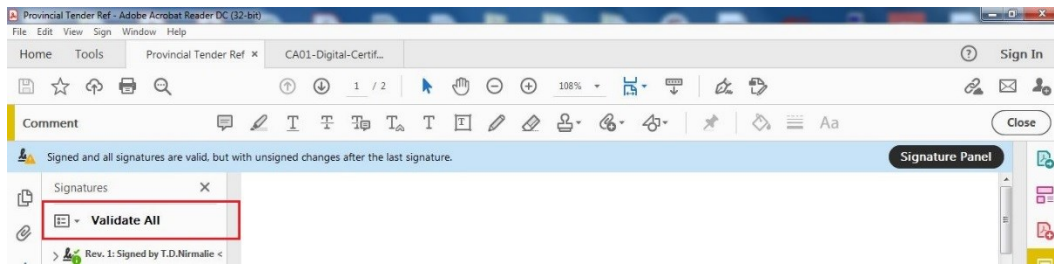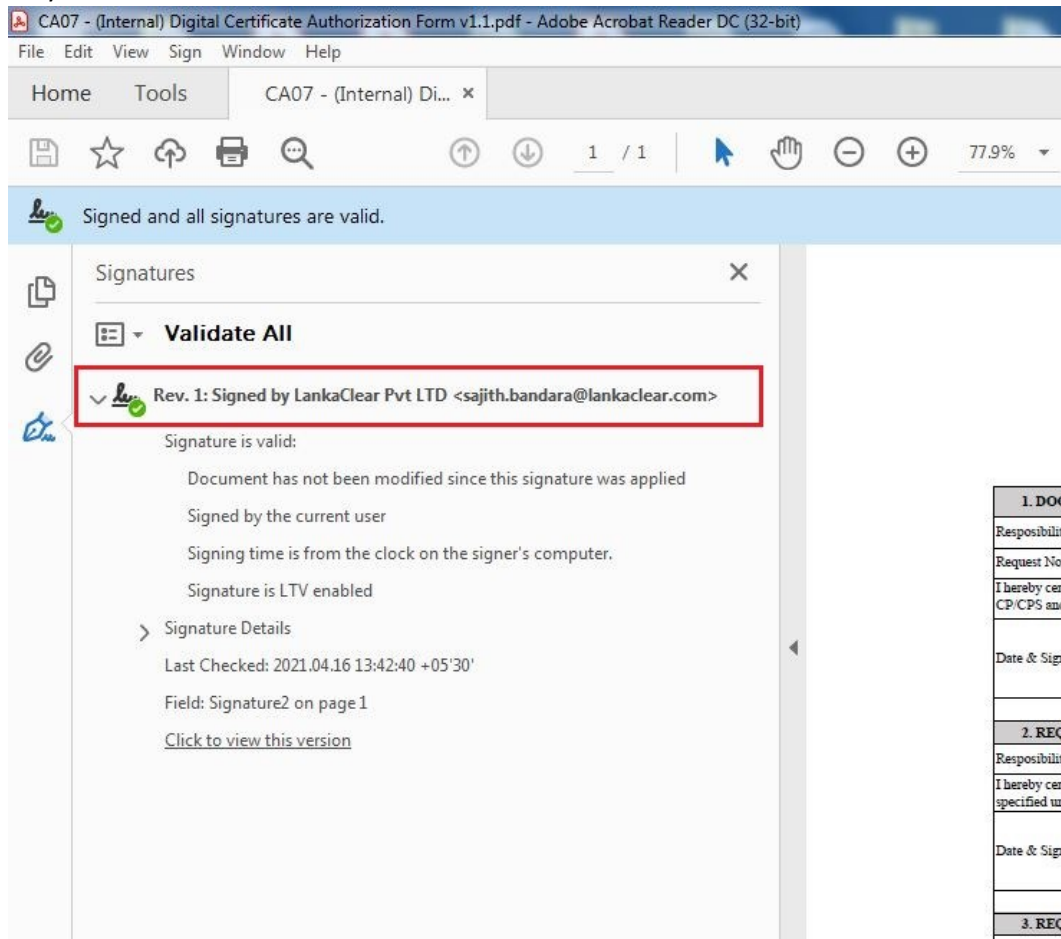


5. Tick on Do not show this message again → Click on Ok.



6. Click on Ok.

7. Click on drop down arrow under each signature and check the validity of the certificate. Proceed only if the certificate is valid.



**Notes**

It's recommended to consider the document as invalid if there are subsequent changes to the document after it's signed.

**How to Check the Validity of Digitally Signed Word and Excel Documents:**

**Note:**

Digital signatures can't be created or removed in Microsoft Excel Starter 2010 or Microsoft Word Starter 2010.

1. Make sure your PC/laptop is connected to the internet
2. Open the Word or Excel Document file that contains the digital signature you want to view.
3. Click **File** > **Info** > **View Signatures**.
4. In the list, on a signature name, click the **down-arrow**, and then click **Signature Details.**
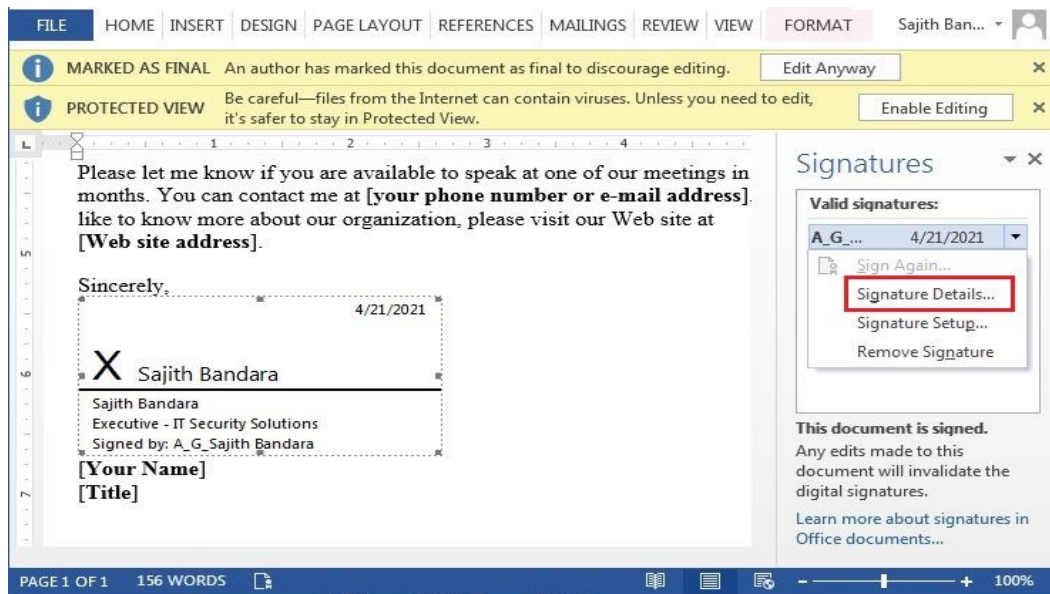


5. From the **Signature Details** dialog box, you can determine the **signature status**
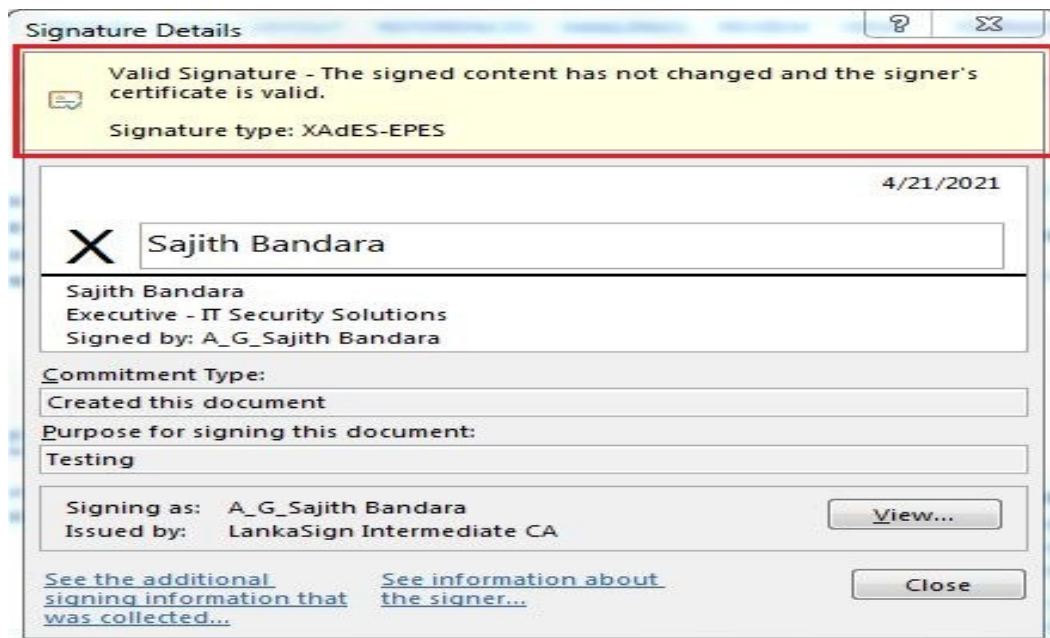
**Status of the Signature in Word and Excel.**

➡ **Valid :-**

The certificate is trusted and isn't expired or revoked. The signed content has not changed and the signer's certificate is valid.

➡ **Invalid :-**

The certificate is revoked or the content signed has been altered.

➡ **Recoverable error :-**

The signature isn't valid now but you might be able to make it valid. The problem might be that you are offline, the certificate is expired, or the certificate issuer isn't trusted.

➡ **Partial signature :-**

A portion of a file is signed.