# Trust Another User's Certificate for Adobe Pro XI or Adobe Reader XI User Guide
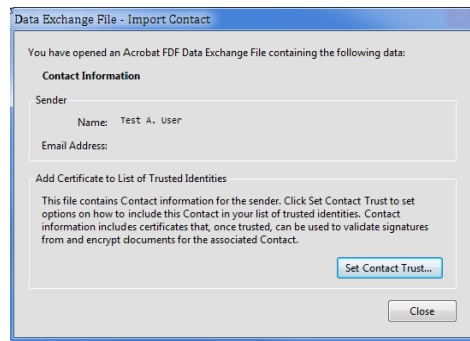
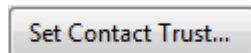1. Open the Certificate Listing on the [eConstruct Portal Site](#)



2. Click on View under Certificate for the User Certificate you want to Trust.

3. One of two dialogue windows will open

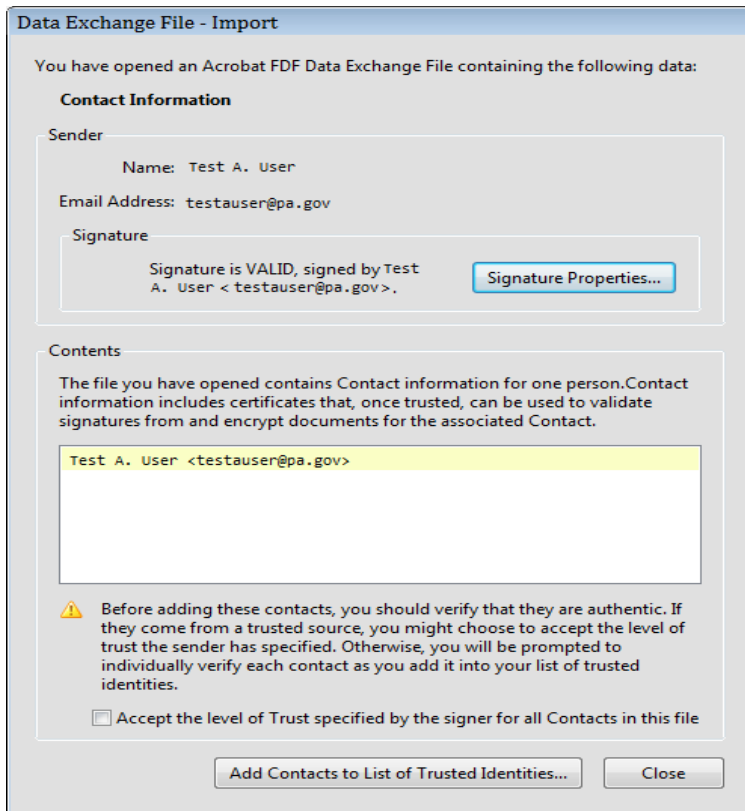    a. If the Data Exchange File – Import Contact Dialogue opens:

    

        i. Click on the Set Contacts Trust…Button.

        

        ii. Proceed to Step 4

    b. The Data Exchange File – Import Dialogue window opens:

**Data Exchange File - Import**

You have opened an Acrobat FDF Data Exchange File containing the following data:

**Contact Information**

Sender

  Name:  Test A. User

Email Address:  testauser@pa.gov

Signature

Signature is VALID, signed by Test A. User < testauser@pa.gov >.

[Signature Properties...]

Contents

The file you have opened contains Contact information for one person. Contact information includes certificates that, once trusted, can be used to validate signatures from and encrypt documents for the associated Contact.

Test A. User <testauser@pa.gov>

⚠ Before adding these contacts, you should verify that they are authentic. If they come from a trusted source, you might choose to accept the level of trust the sender has specified. Otherwise, you will be prompted to individually verify each contact as you add it into your list of trusted identities.

☐ Accept the level of Trust specified by the signer for all Contacts in this file

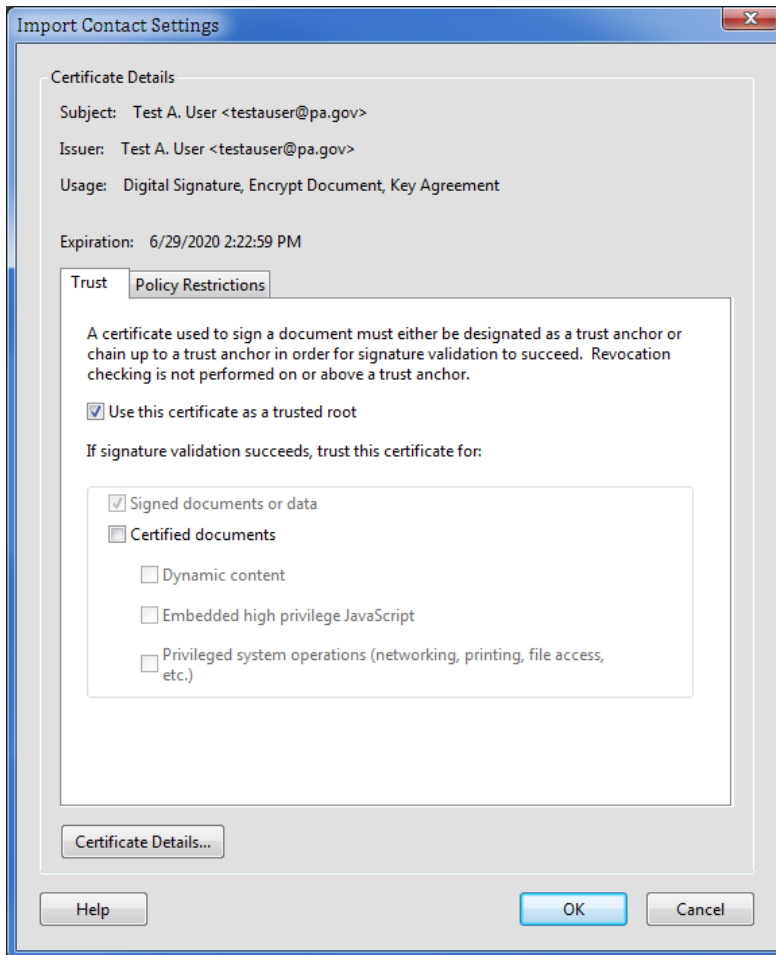[Add Contacts to List of Trusted Identities...]  [Close]

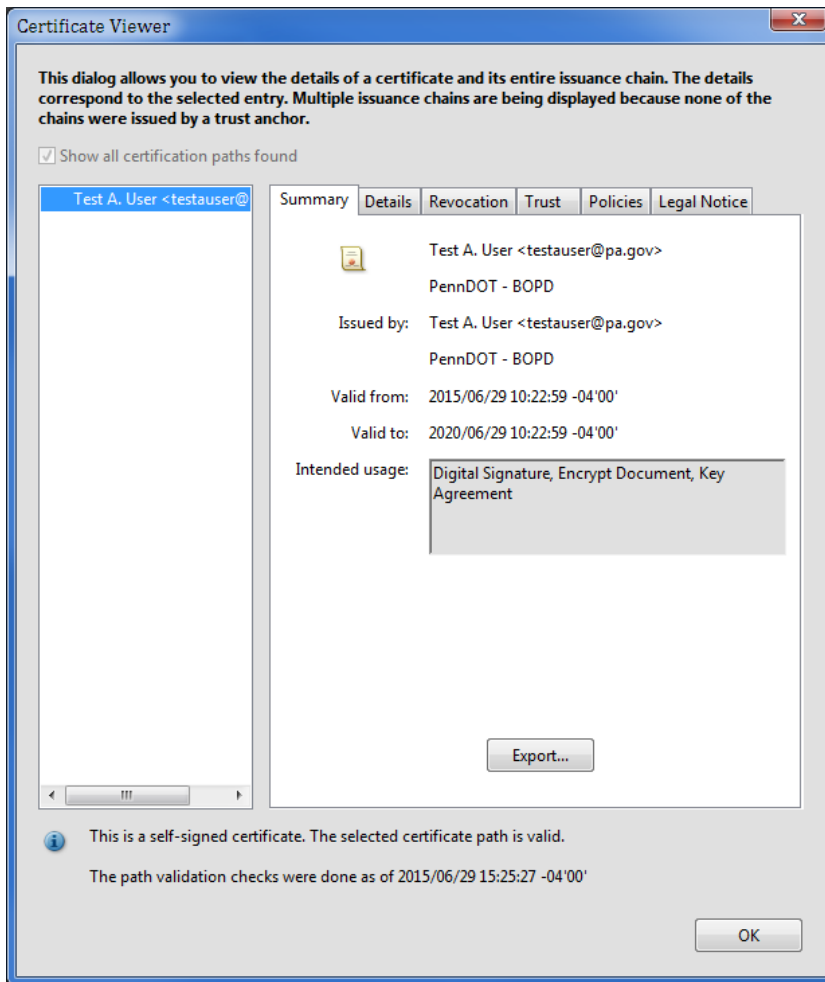     i. Click on the Add Contacts to List of Trusted Identities Button.

[Add Contacts to List of Trusted Identities...]

     ii. Proceed to Step 4
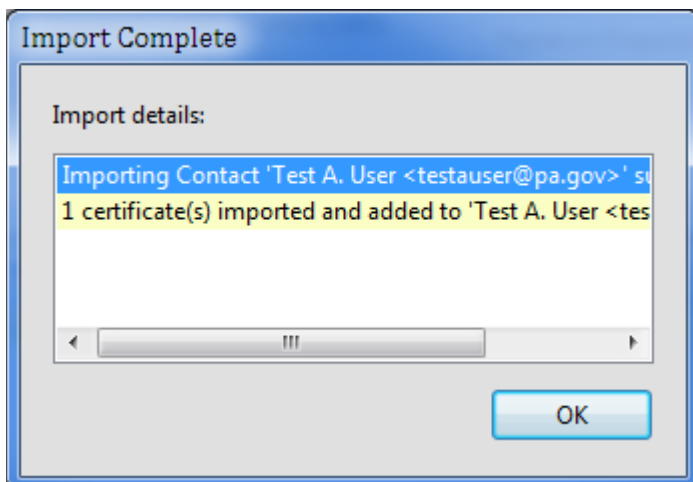
4. Select the box Use this certificate as a trusted root to accept the certificate

Pennsylvania
DEPARTMENT OF TRANSPORTATION

## Import Contact Settings

### Certificate Details

Subject:  Test A. User <testauser@pa.gov>

Issuer:  Test A. User <testauser@pa.gov>

Usage:  Digital Signature, Encrypt Document, Key Agreement

Expiration:  6/29/2020 2:22:59 PM

**Trust** | Policy Restrictions

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.)

[ Certificate Details... ]

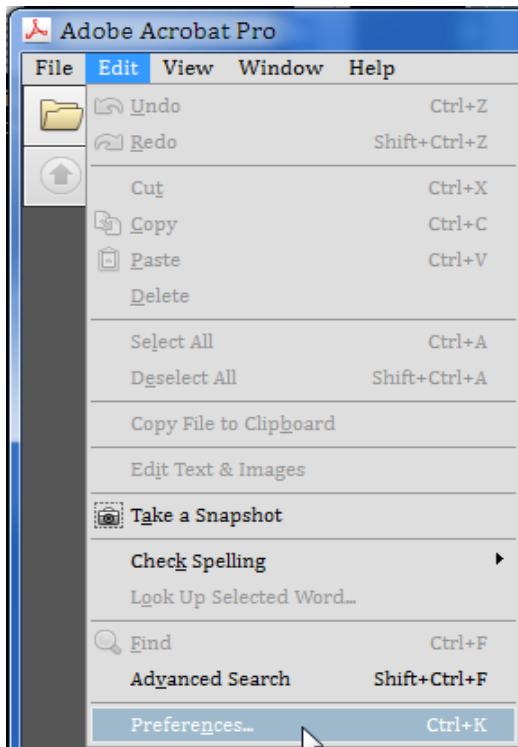[ Help ]                    [ OK ]   [ Cancel ]

5. Click the Certificate Details Button to review the certificate.



6. Click the Ok button to accept the certificate. A window will open and display the results of the import.



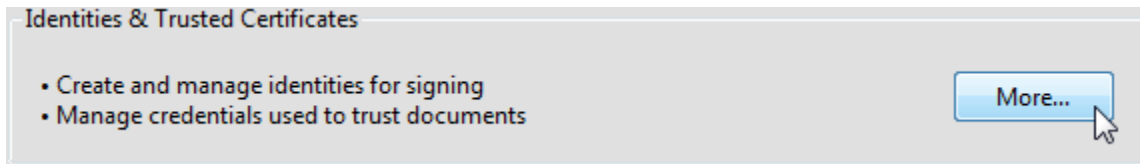IT Service Desk number (717) 783-8330 or toll free (855) 783-8330

7.  Click the Ok button to close this window.

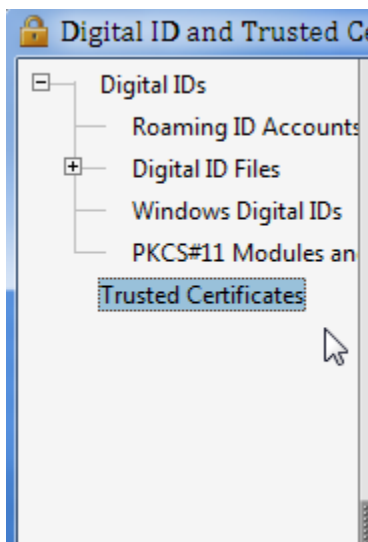8.  To review the accepted certificates, select Preferences from the Edit Menu.



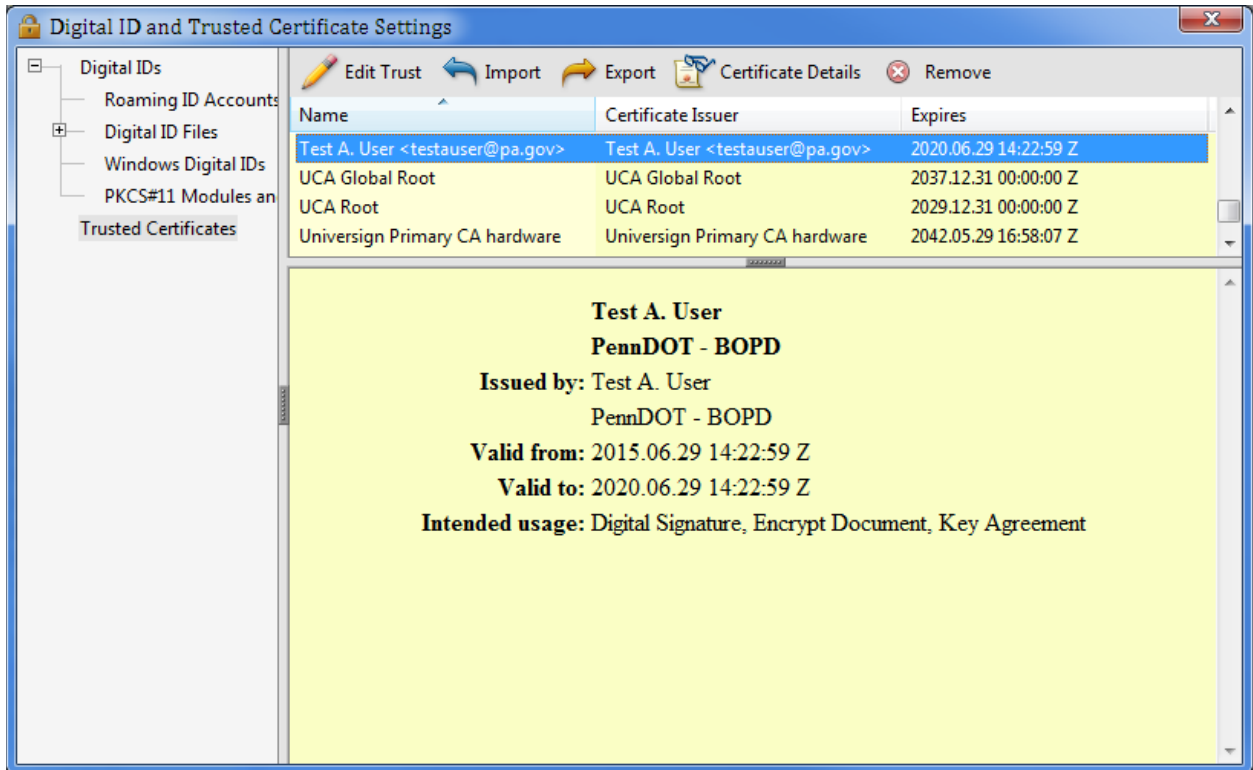9.  Scroll and click on Signatures under Categories.
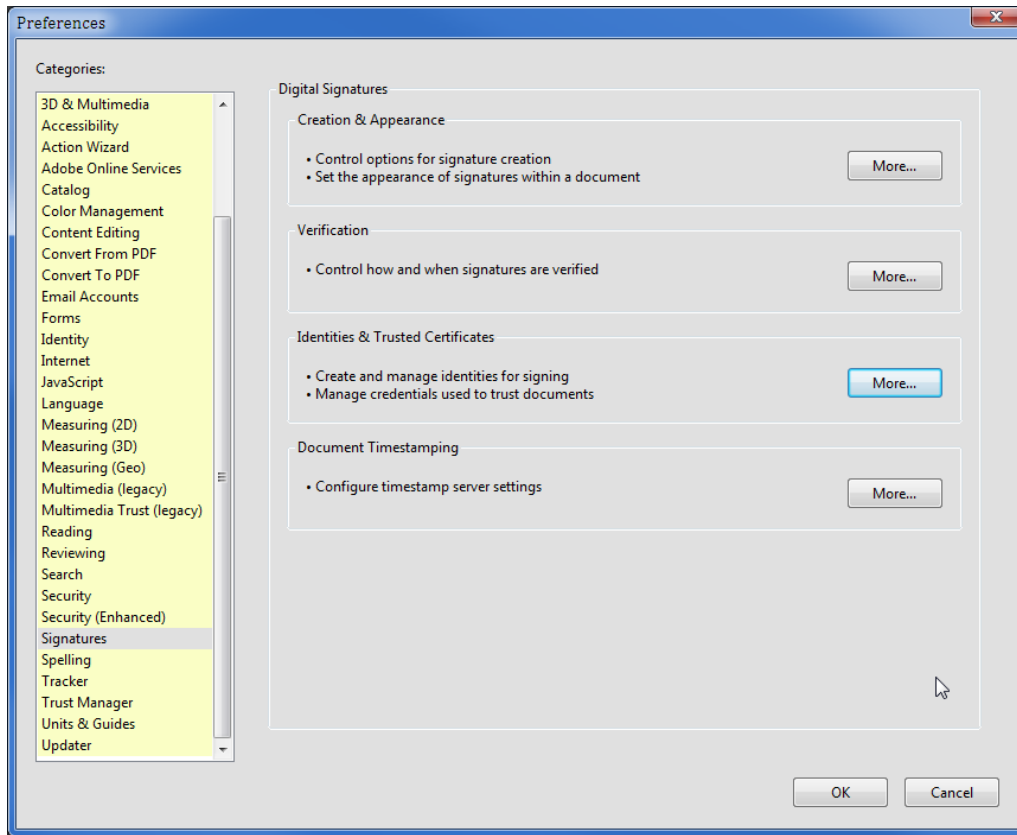
10. Click the on the More…. Button in the Identities & Trust Certificates section.



11. Click on Trust Certificates in the panel

12. The window will show all trust certificates and the associated data, if selected.  Click the [X] to close the window.

13. Click the Ok Button to close the Preferences window.