

OFFICE OF THE CHIEF INFORMATION OFFICER
INNOVATIONS & OPERATIONAL ARCHITECTURE

User Guide for Digital Signatures in Adobe Acrobat 8.x and 9.x

21 March 2011



United States
Department of
Agriculture

Table 1. Document Revision & Version Information

| Version No. | Date | Description | Author/Approval |
|-------------|-----------|-----------------|-------------------------------|
| 1.0 | 3/21/2011 | Version 1 Final | Todd Kaywood, Carol Van Natta |

Digital Signatures Adobe Acrobat 8 & 9.docm

Table of Contents

| | |
|---|-----------|
| 1. Introduction | 4 |
| 1.1 What is a Digital Signature? | 4 |
| 1.2 When Should I Use a Digital Signature..... | 4 |
| 1.3 Definitions and Acronyms | 5 |
| 2. Adding a Digital Signature to an Adobe Acrobat 8.x Document | 6 |
| 2.1 How to Digitally Sign a Document..... | 6 |
| 2.2 How to Remove a Digital Signature..... | 18 |
| 2.3 How to Verify a Digital Signature | 20 |
| 3. Adding a Digital Signature to an Adobe Acrobat 9.x Document | 22 |
| 3.1 How to Digitally Sign a Document..... | 22 |
| 3.2 How to Remove a Digital Signature..... | 29 |
| 3.3 How to Verify a Digital Signature | 30 |
| 4. Help Desk and Troubleshooting for Digital Signature | 33 |
| 5. References | 34 |

1. Introduction

This document provides instructions on how to add digital signatures to Adobe Acrobat version 8.x and version 9.x documents. You must have an activated LincPass + PIN, the ActivIdentity ActivClient software installed, and a card reader to digitally sign a document. You must also have Adobe Acrobat version 8.x or version 9.x installed.

NOTE: These instructions are based on the FDCC-approved installation of Adobe Acrobat on computers with the Windows XP operating system. As other agencies may have implemented options, settings, and limitations during installation, you may see slight variations in behavior and screenshots than those shown in this document. Check with your agency's IT help desk if you have questions or problems.

User guides like this one are also available for:

- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Outlook 2003 and 2007 (for sending digitally signed emails)

1.1 What is a Digital Signature?

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document. Besides being easily transportable, it can also add assurance that the content of the message or document that has been sent is unchanged. When time-stamped, the ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

Digital signatures provide a high form of signature and content integrity. Digital signatures are based on public key infrastructure (PKI), and are a result of a cryptographic operation that guarantees signer authenticity, data integrity, and non-repudiation of signed documents. The digital signature cannot be copied, tampered, or altered, and therefore non-repudiable. In addition, because they are based on standard PKI technology, digital signatures made within one application (such as Microsoft Word or Adobe Acrobat) can be validated by others using the same application.

1.2 When Should I Use a Digital Signature

USDA is developing policy or directives that will officially address the technology of digital signature and its application in USDA. Check with your agency for interim guidance on when to use digital signatures for business purposes. Here are some general guidelines on when you might want to use them:

- Placing a "seal" on the document. Digitally signing using the USDA LincPass card is assurance of document integrity and its legal standing as an official document.
- Multiple signatures. Documents can be digitally signed by more than one person, indicating an approval or agreement with the (unaltered) content.
- Compliance. A digital signature may be required for compliance purposes when a legal signature is required. For example, the System Security Plan for a major system must be signed by the system owner and by the responsible security officer.

- Leadership Memorandums and Policy Issuance. Digital signatures on such documents are assurance that the document was reviewed and approved by the signer, and the recipient can be assured the content is as the signer intended.
- Verification of the signer's digital identity. Digital signatures can be traced to a known electronic identity, which in turn represents a specific individual in USDA. For example, although email headers can be spoofed or forged, the digital signature associated with it cannot.

This is by no means an exhaustive list, and Agencies may well find other uses for digital signatures that meet a specific business need.

1.3 Definitions and Acronyms

- **PIV card:** FIPS 201-compliant personal identity verification (PIV) card.
- **LincPass:** USDA's name for the PIV cards it issues to employees, contractors, partners, affiliates, et al.
- **HSPD-12:** Homeland Security Presidential Directive 12, signed 27 August 2004. HSPD-12 requires all federal agencies to conduct background investigations and issue personal identity verification (PIV) credentials to all employees and contractors, and integrate those credentials with logical and physical access control systems.
- **Microsoft Office file types:**
 - DOC file: Microsoft Word 2003 file
 - DOCX file: Microsoft Word 2007 file (*not backward compatible with Word 2003*)
 - DOCM file: Microsoft Word 2007 file (*not backward compatible with Word 2003*)
 - XLS file: Microsoft Excel 2003 file
 - XLSX file: Microsoft Excel 2007 file (*not backward compatible with Excel 2003*)
 - PPT file: Microsoft PowerPoint 2003 file
 - PPTX file: Microsoft PowerPoint 2007 file (*not backward compatible with PowerPoint 2003*)
 - PDF file: Adobe Acrobat version 8 & 9
 - Microsoft Outlook 2003
 - Microsoft Outlook 2007
- **User:** Employee, contractor, affiliate, partner, et al. with an activated LincPass card.
- **Public key infrastructure (PKI):** Standards-based system that creates a hierarchy of "certification authorities" to allow individuals and organizations to identify each other for the purpose (principally) of doing business electronically.
- **Non-repudiation:** A method to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. In reference to digital security, non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message.

2. Adding a Digital Signature to an Adobe Acrobat 8.x Document

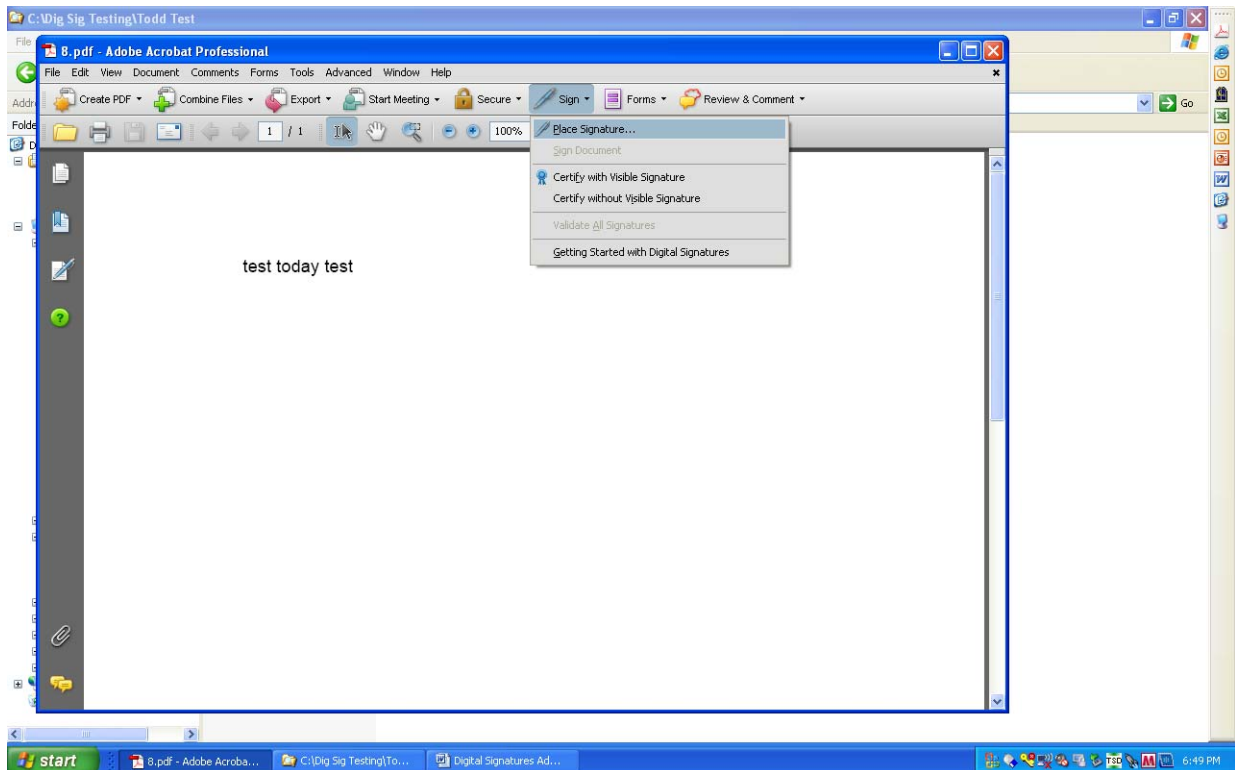
NOTE: Adding digital signatures to Acrobat 8.x documents can be done, but it takes many steps that must be repeated each time, and Acrobat 8.x lacks digital signature information and performance. If you will be using digital signatures regularly for your business tasks, you should, if at all possible, upgrade to Adobe Acrobat 9.x, as it will improve verification, performance, and ease of use, and therefore your productivity.

2.1 How to Digitally Sign a Document

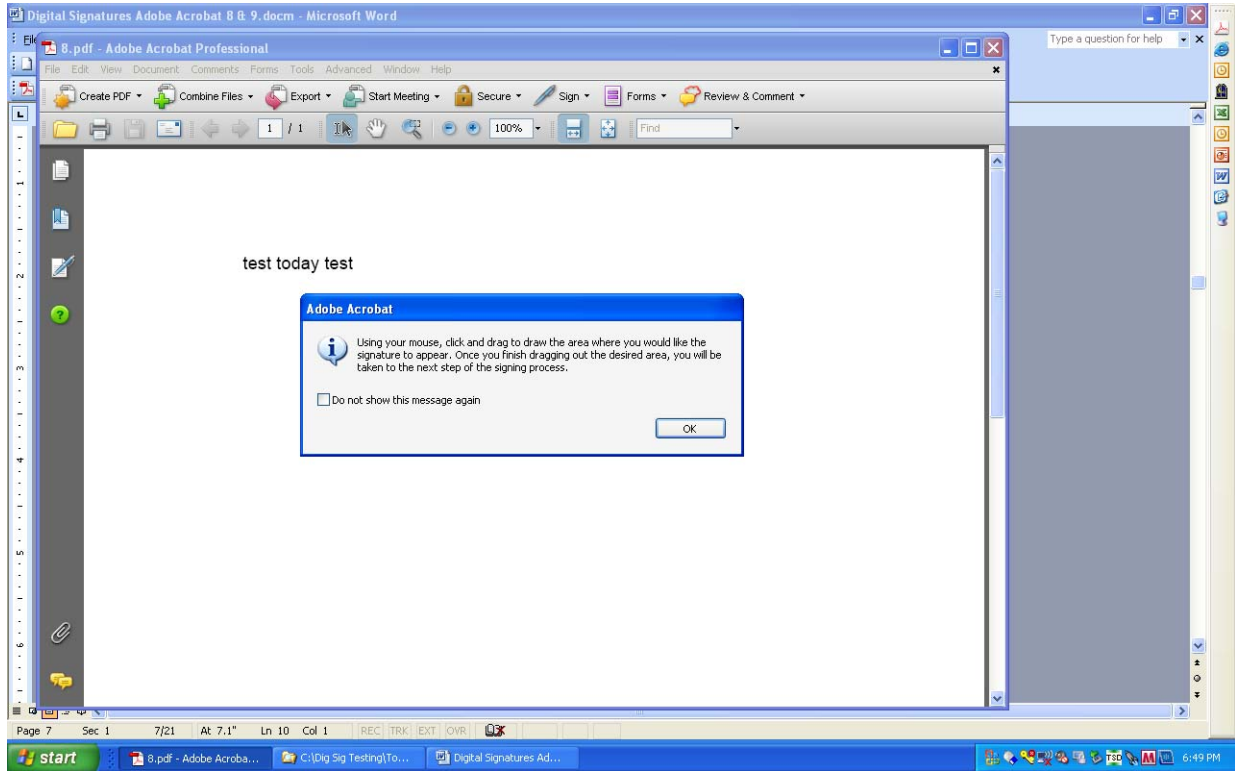
1. Insert your LincPass into the computer's card reader.



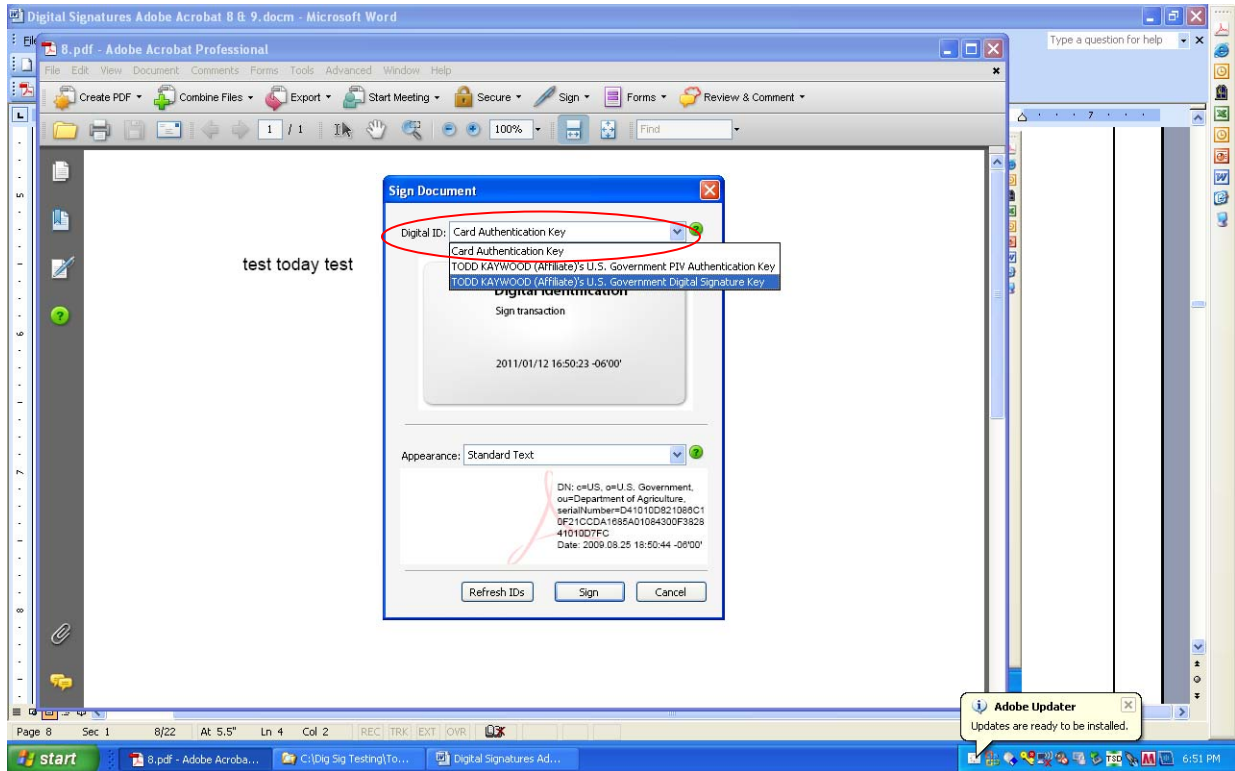
2. Open Adobe Acrobat. Either create a new document or open an existing document you want to sign.
3. From the top menu, select **Sign**, then **Place Signature**.



4. Adobe will instruct you to draw an area on the screen where you want to place the signature. Click the **OK** button, then with your mouse, draw a box for the signature. You can set the size of the signature, but it's easier to read if you make it as large as possible. You can place the signature anywhere in your document as well, but the recommended locations are at the beginning or the end of the document.



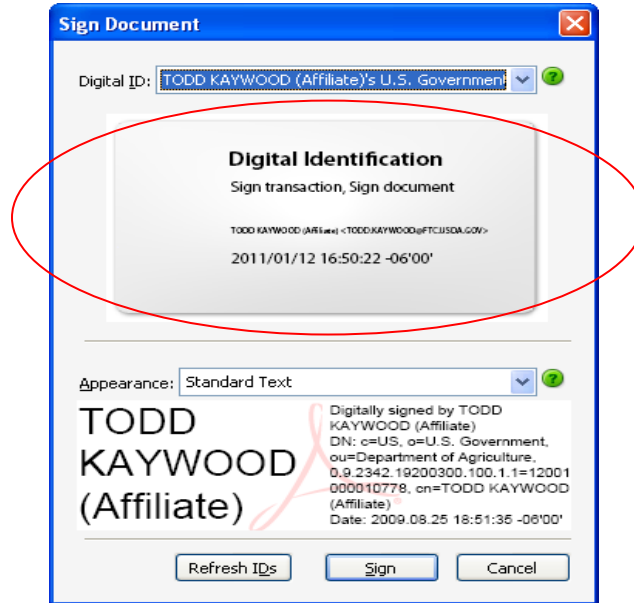
5. After you have created the signature box, a “Sign Document” window appears. From the Digital ID droplist, select the certificate for Digital Signature.



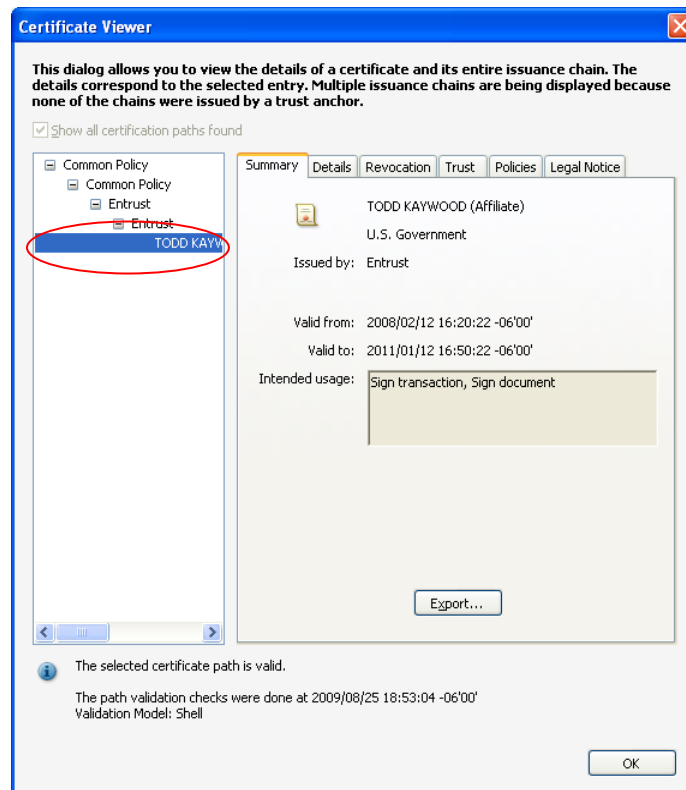
NOTES:

1. If other people with LincPass cards have used your computer, you may see their certificates offered in this list. Only select your personal certificates.
2. If you don't see your certificate keys listed at all, first check that your card is in the reader and wait a minute or two for Acrobat to find it. If your keys still aren't listed, your agency may need to implement the Adobe Technical Modification for Digital Signature. Please ask your system administration or help desk team to work with OCIO-IOA's technical point of contact for help implementing this modification. The technical modification will also save you from having to make this selection each time you want to digitally sign a document.

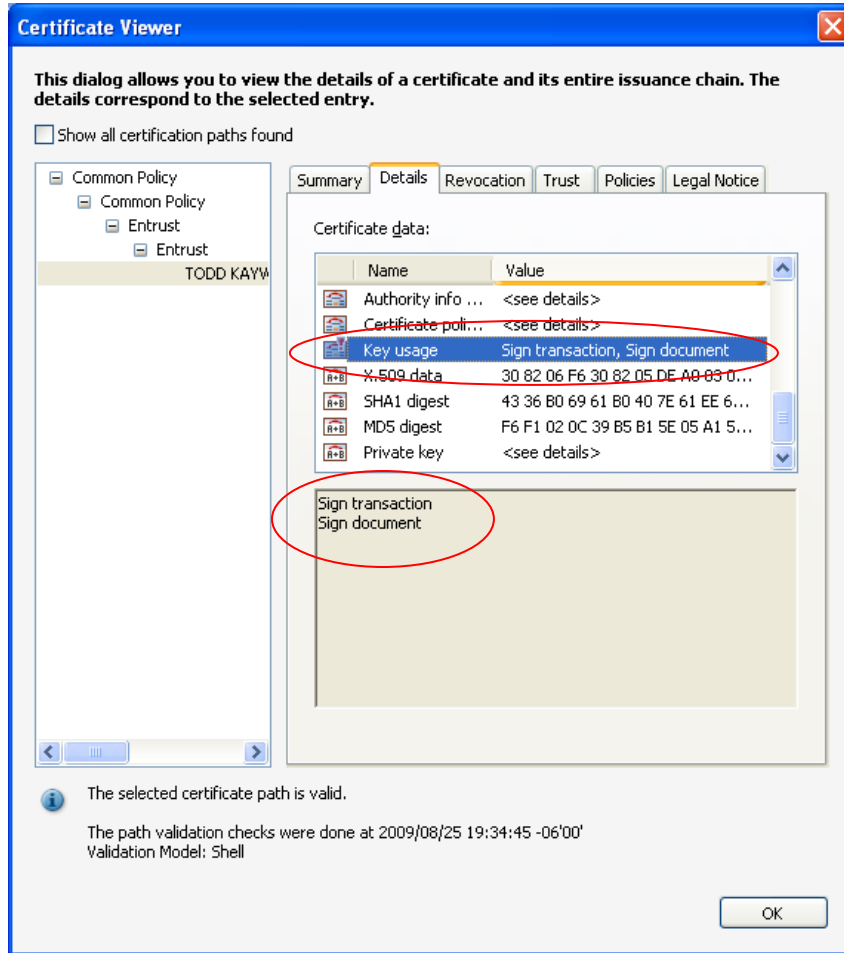
6. Because the “Digital ID” droplist isn’t very helpful in describing the certificates, you’ll need to view the certificate to confirm it is the correct certificate to use for signing.
7. Select one of the two lines with your name, then double click the large rectangle that says “Digital Identification.” For most certificates, the correct one will be one with your name but *without* the “Gov. PIV Auth. Key” label.



8. In the Certificate Viewer window, open items in the left-side menu until you get to the lowest level. Click to highlight your name.



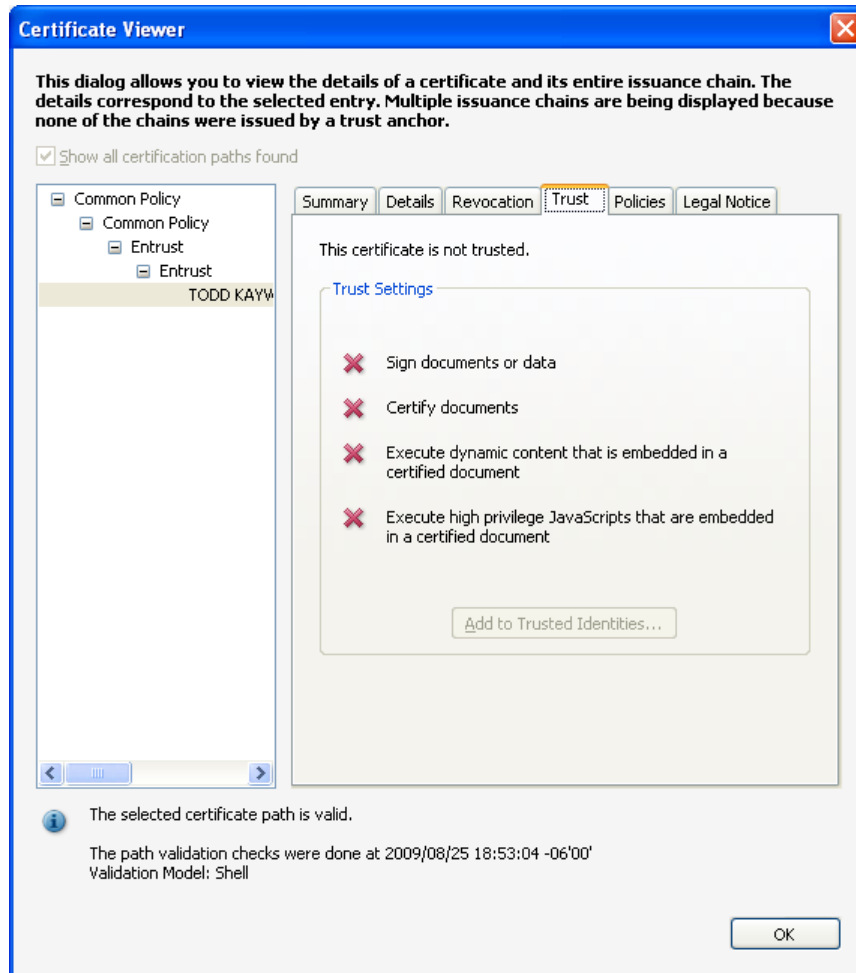
9. Click the “Details” tab, then in the right-hand window, scroll down to the “Key usage field.”



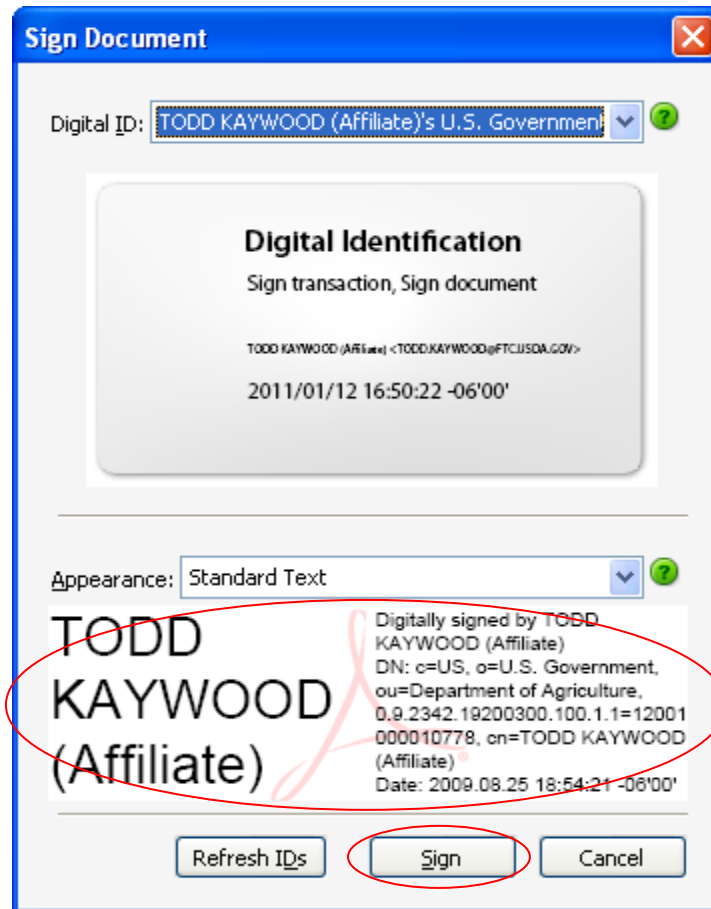
You want the certificate that says “Sign transaction, Sign document” in the Key usage value column. Click the **OK** button to close the window.

If you don’t see the correct key usage value, go back to Step 6 and select the other certificate with your name, then repeat steps 7-9.

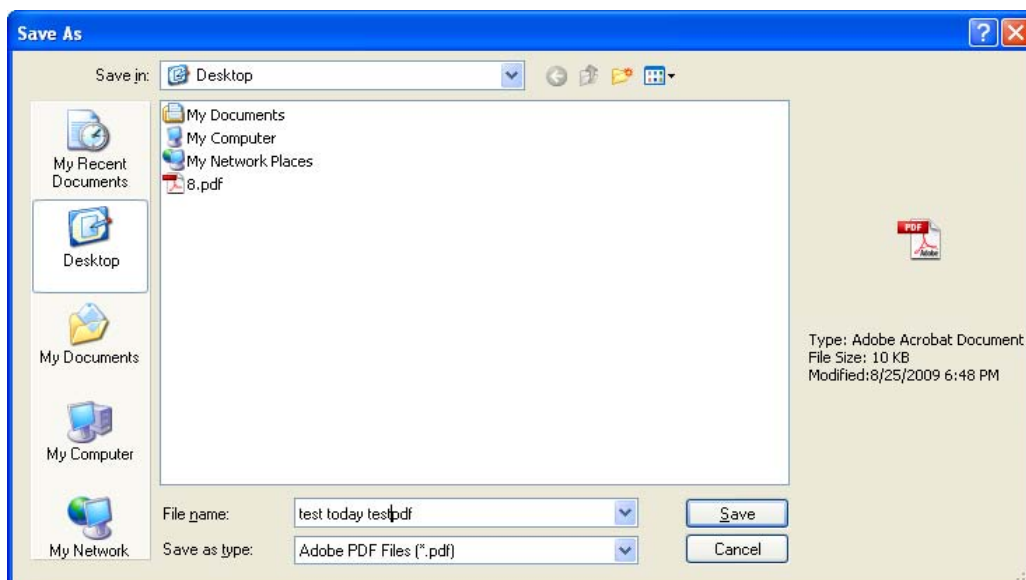
To view the trust level at this point, click the “Trust” tab. It will show there is no trust established yet, which is Adobe’s way of saying the document isn’t signed yet. Click the **OK** button to close the window.



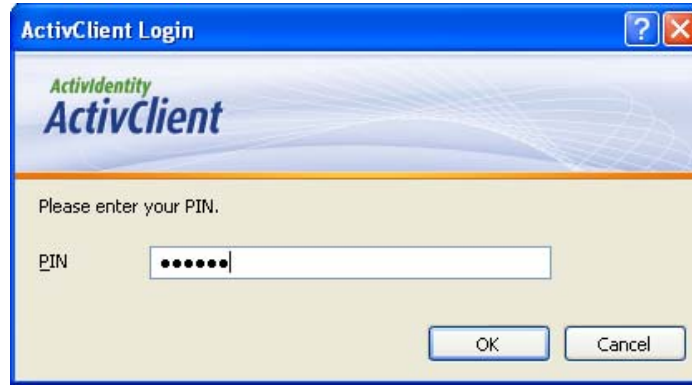
10. The Sign Document window now shows the correct certificate selected in the bottom area. Click the **Sign** button.



11. When Acrobat prompts you, save the file. If you are working with an existing document, you may want to save it with a new name to distinguish it from the unsigned version of the document.

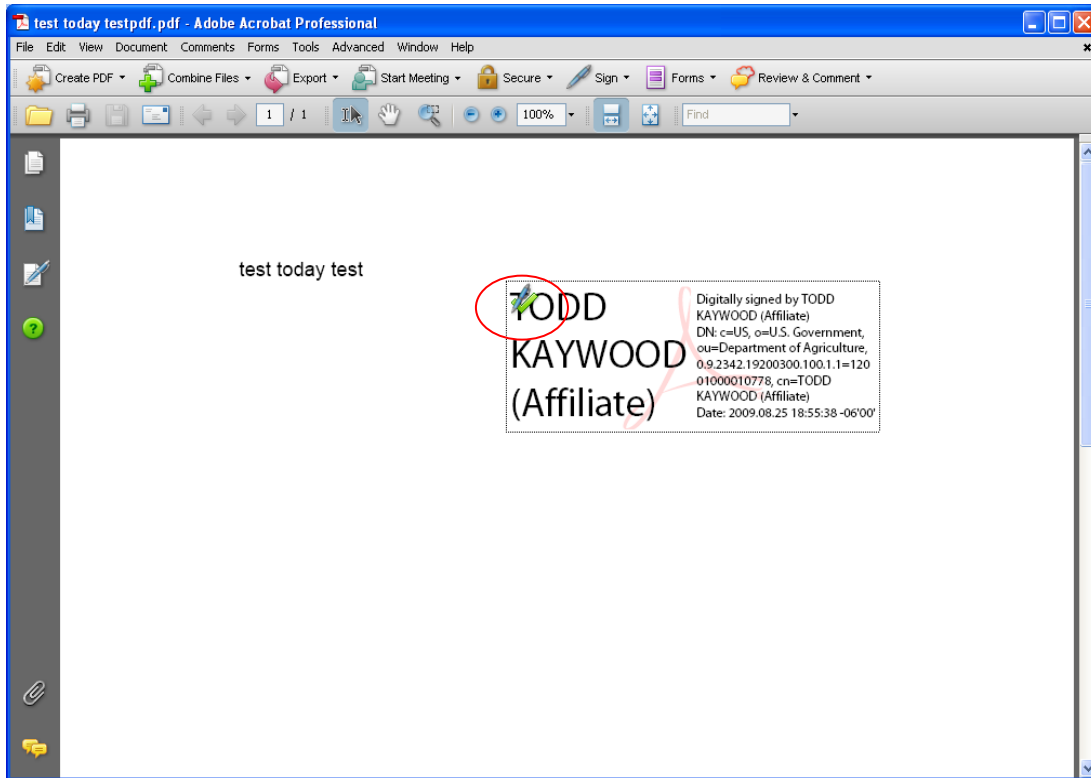


12. At the ActivClient prompt, enter your LincPass PIN, then press ENTER or click the **OK** button.

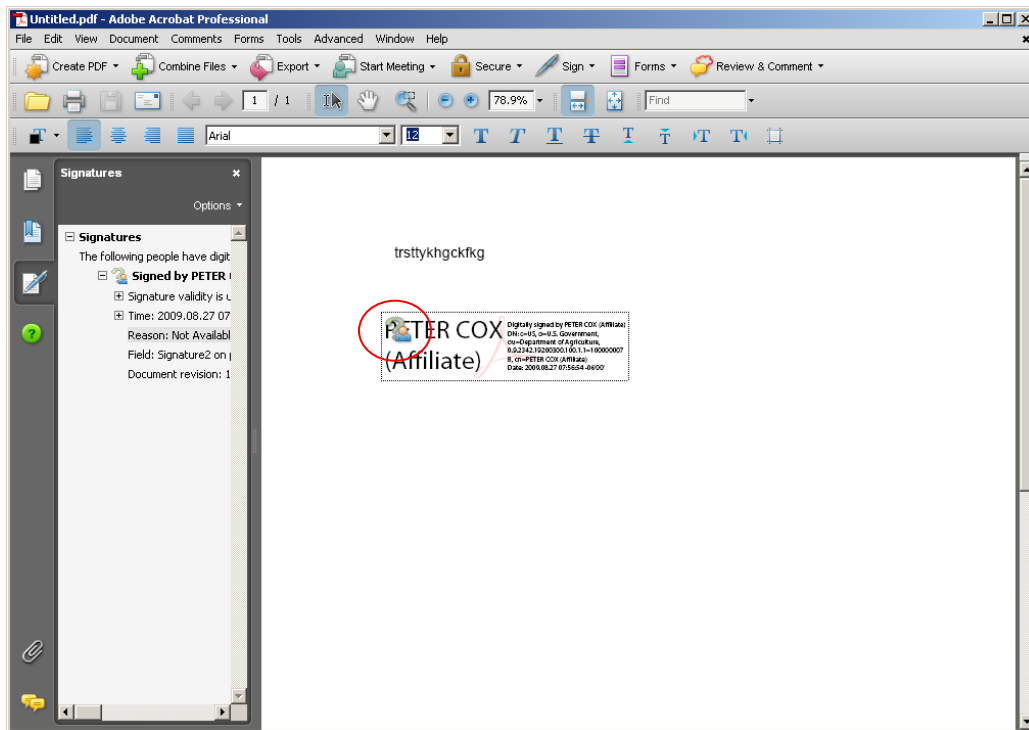


13. Your document is now signed, and you will see the digital signature representation on the document where you placed it. If the signature has a green pencil icon over the name, the signature has a valid trust. If the digital signature block has a question mark over the name, it means the signature still needs to be validated with the trust from the certificates.

Digital signature that is validated with the trust

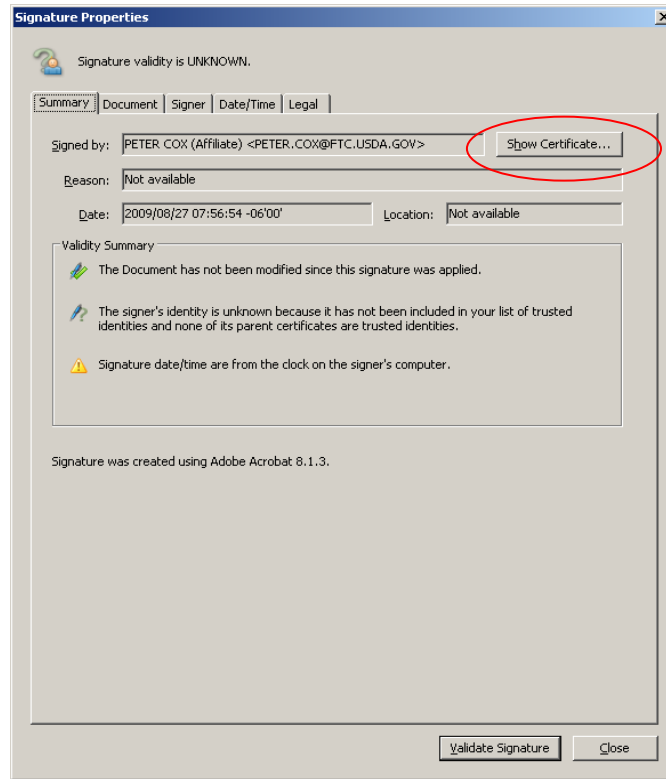


Digital signature that still needs to be validated with the trust

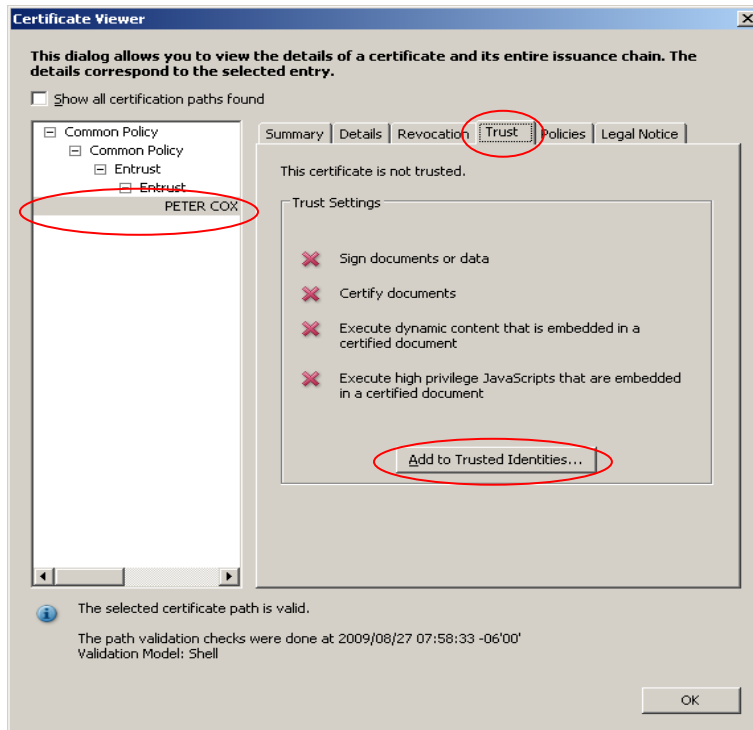


If your signature shows a question mark icon, you must to validate it through Adobe by following steps 14-17. You will only need to do this once; thereafter, you can skip to step 18.

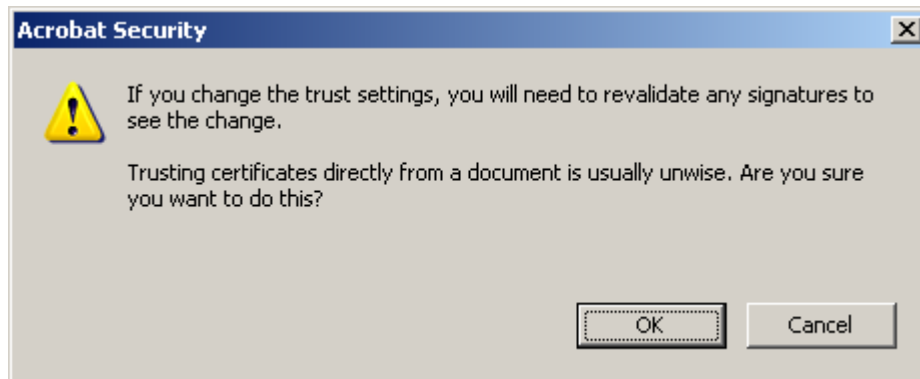
14. Double-click the digital signature in your document to open the Signature Properties window, then click the **Show Certificate** button.



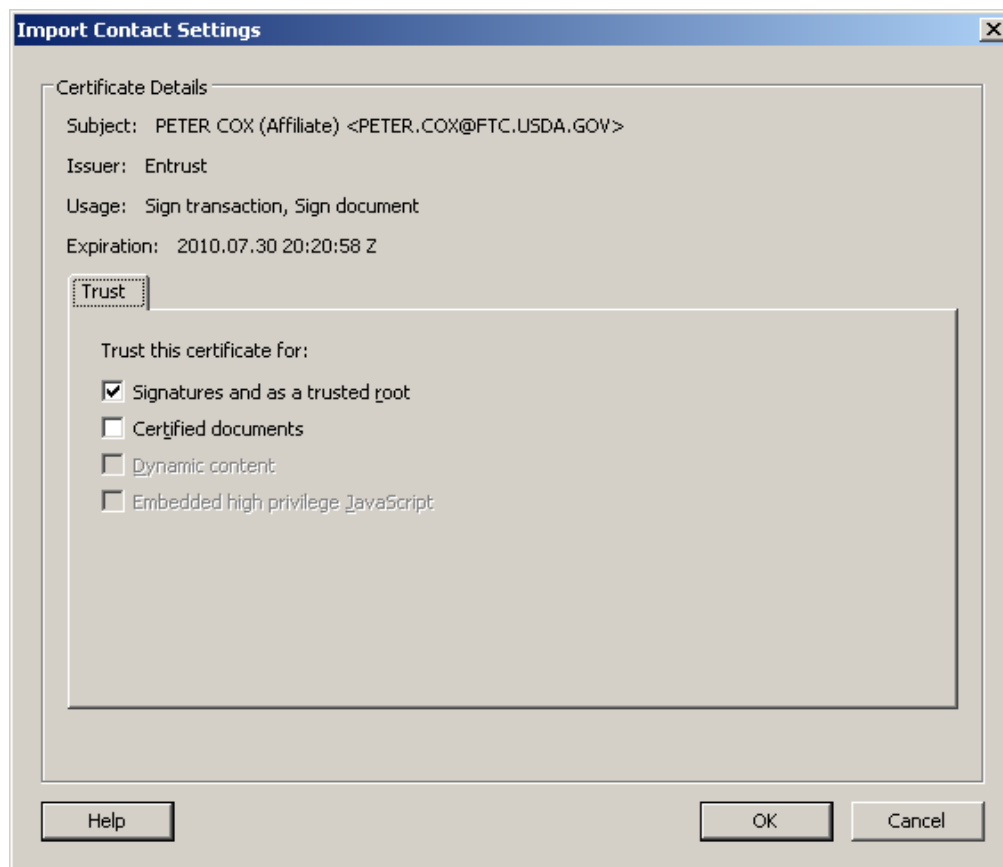
15. Click the Trust tab, then click the hierarchy in the left window to find the certificate with your name. Click the **Add to Trusted Identities** button.



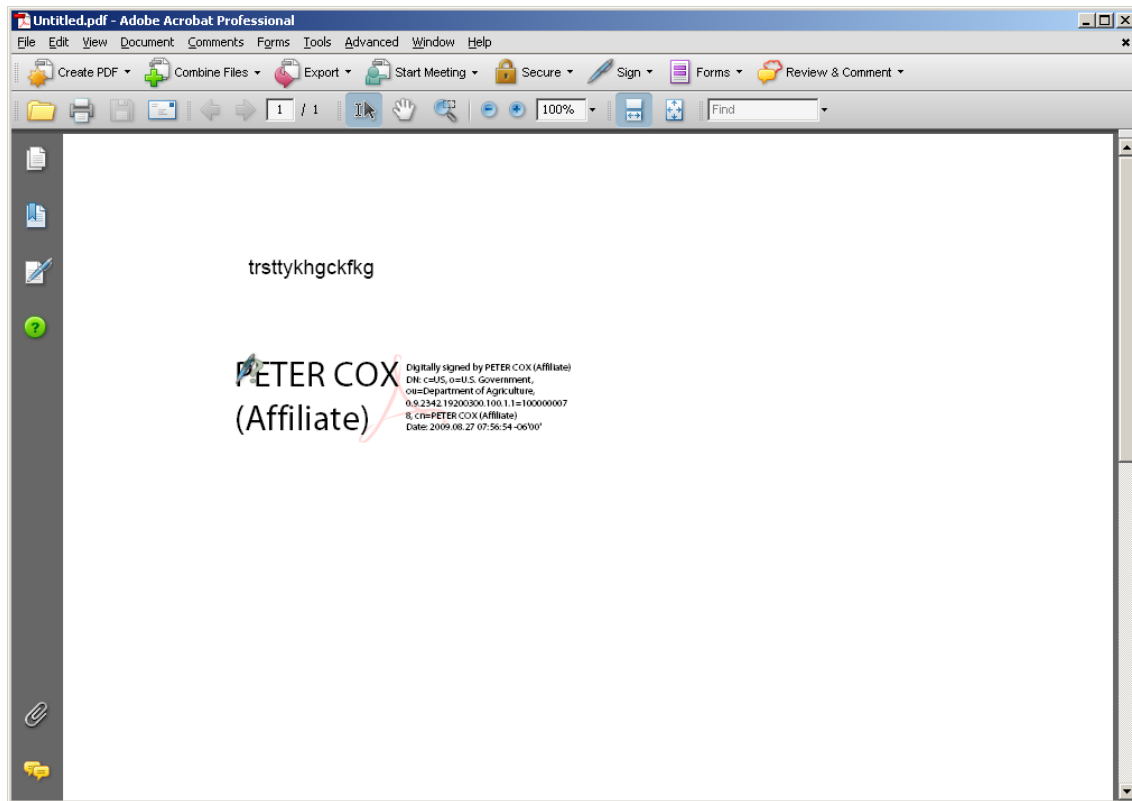
16. Adobe warns you about trusting certificates. Since you are trusting the certificates for your LincPass card, click the **OK** button.



17. In the Import Contact Settings window, make sure the "Signatures and as a trusted root" option is checked, then click the **OK** button.



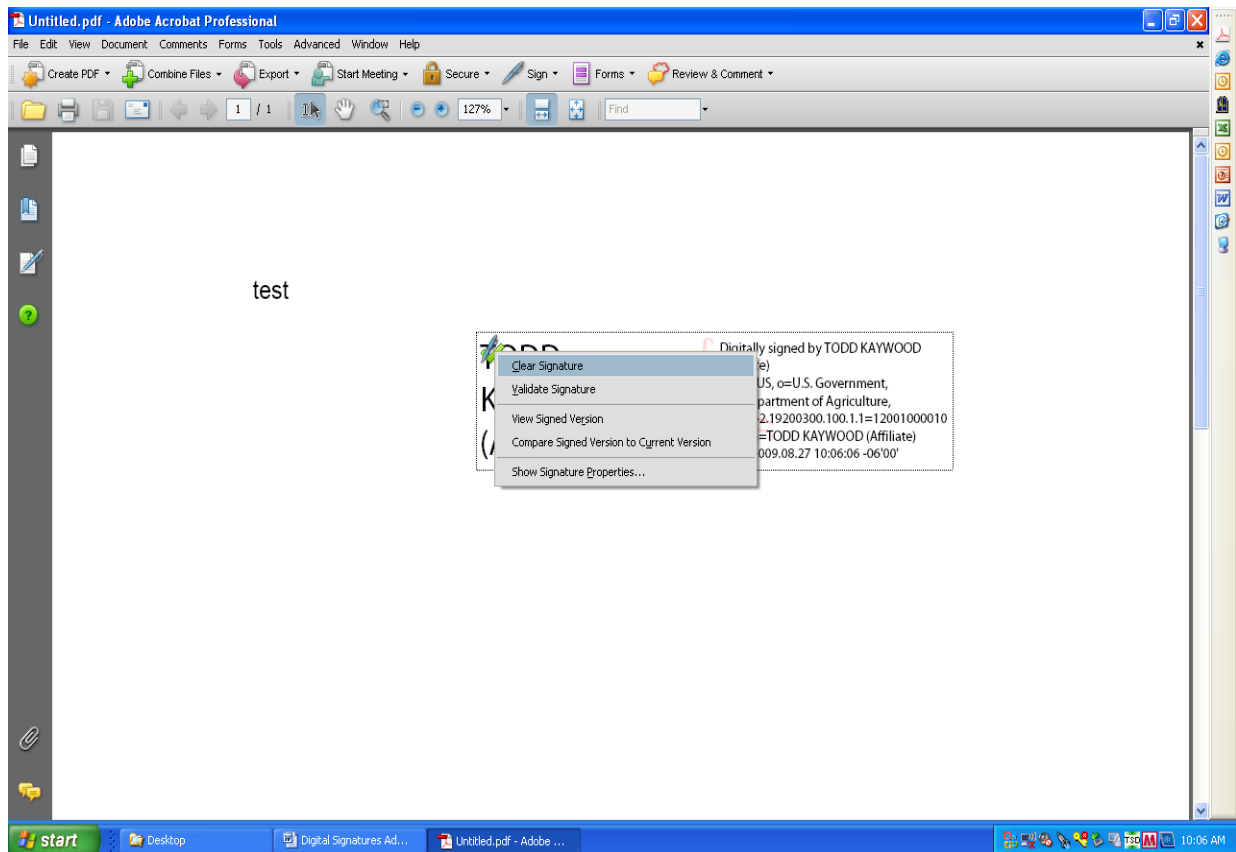
18. Your document is now digitally signed. Close it without making any changes.



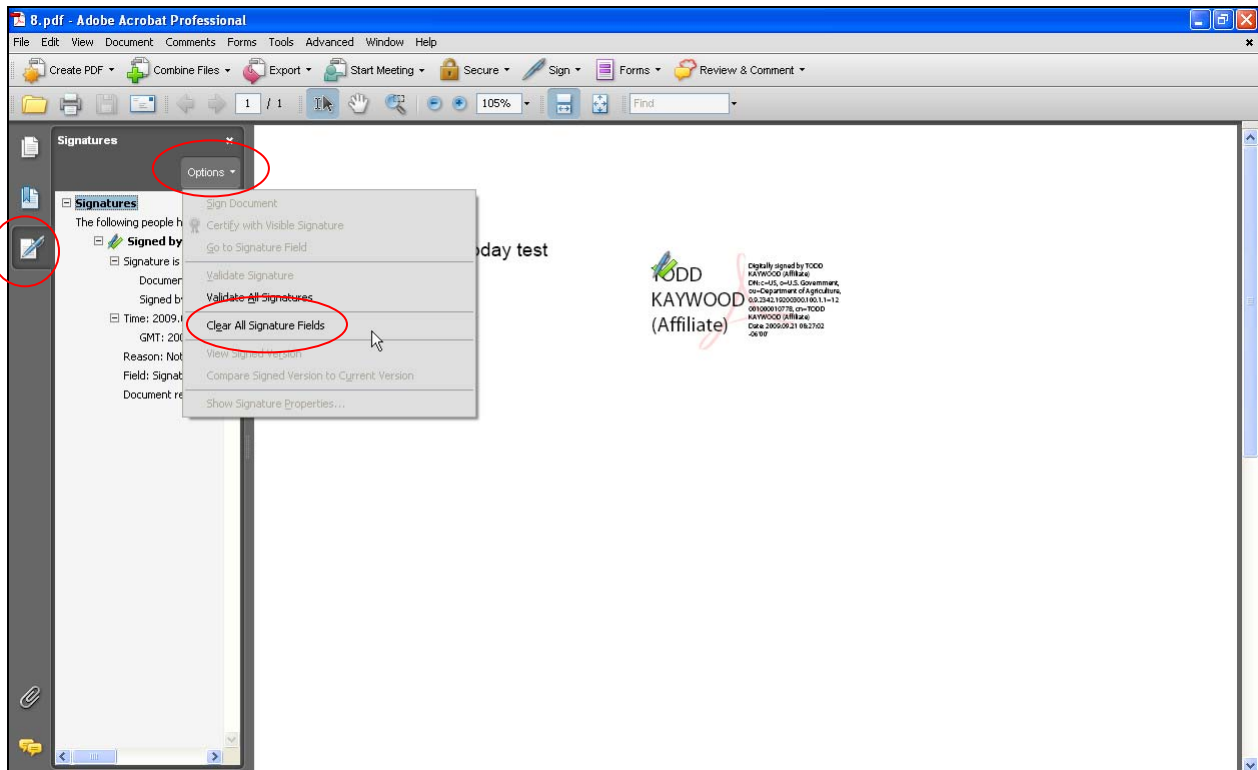
NOTE: Other people can digitally sign the same document by following steps 1-18 in this section. You can have as many people digitally sign the document as needed.

2.2 How to Remove a Digital Signature

1. Open the file from which you want to remove a digital signature.
2. Find the signature block of the signature you want to remove, and right-click to open the context menu. Select the Clear Signature option to remove this signature.



3. If you want to remove all the signatures at once, open the Signatures panel (click the Signature icon in the left-side toolbar). Click the Options tab in the Signatures panel, then select the “Clear All Signature Fields” option.



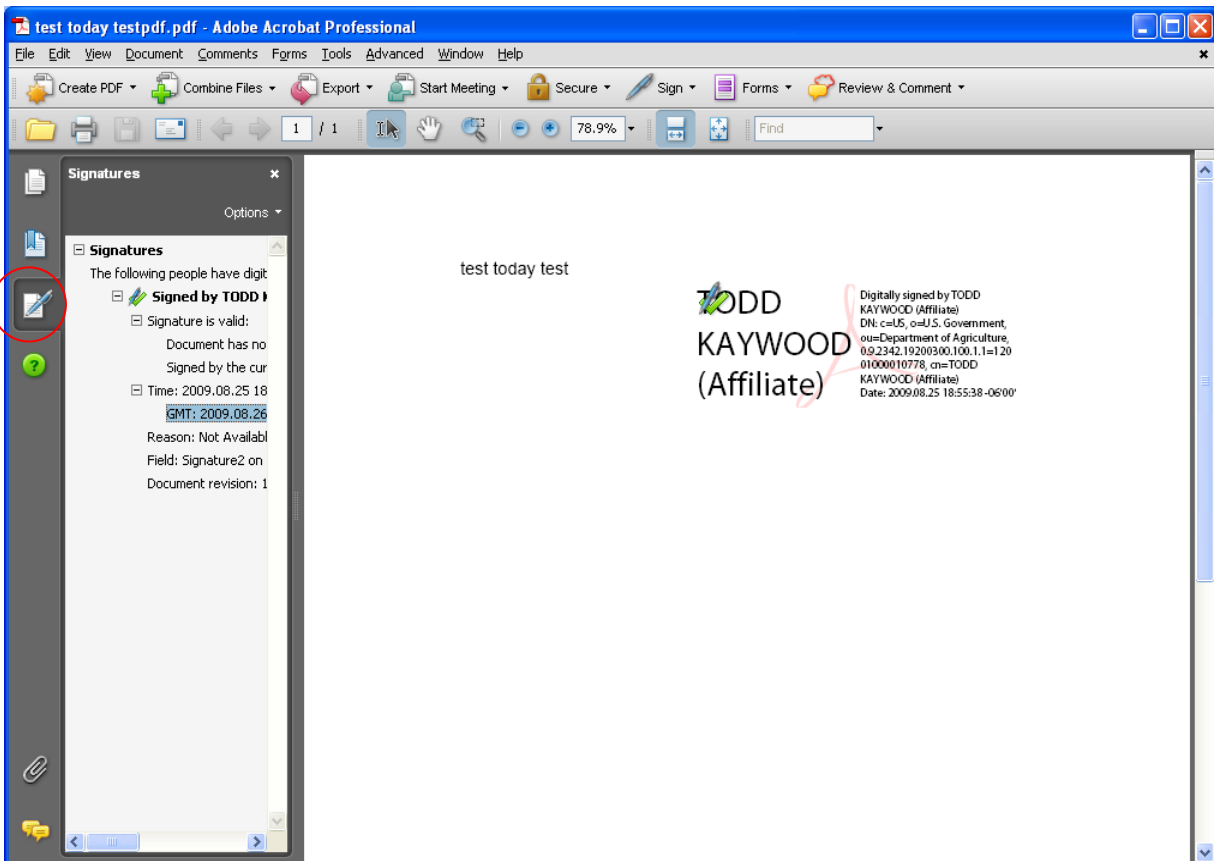
4. Acrobat will warn you that you can't undo this action and ask you to confirm you want to remove the signatures. Click the OK button.



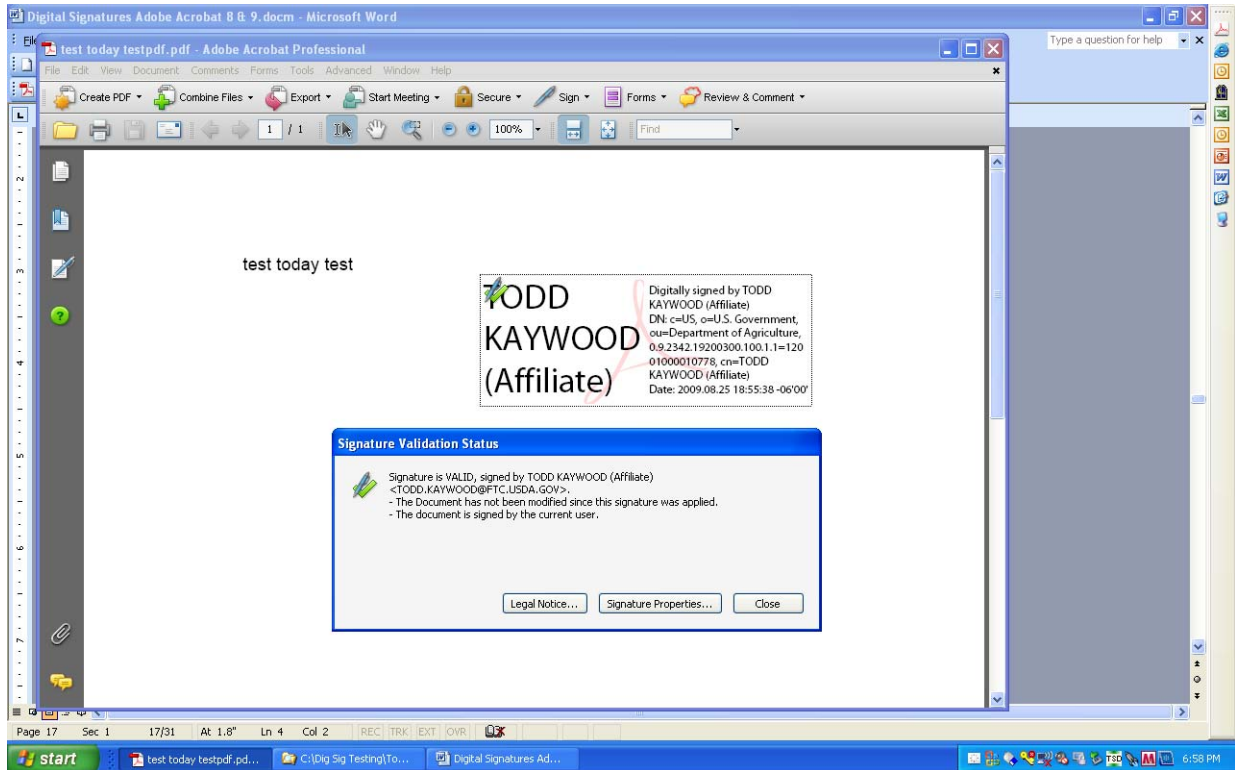
You don't have to save the PDF again, but it won't hurt anything if you do.

2.3 How to Verify a Digital Signature

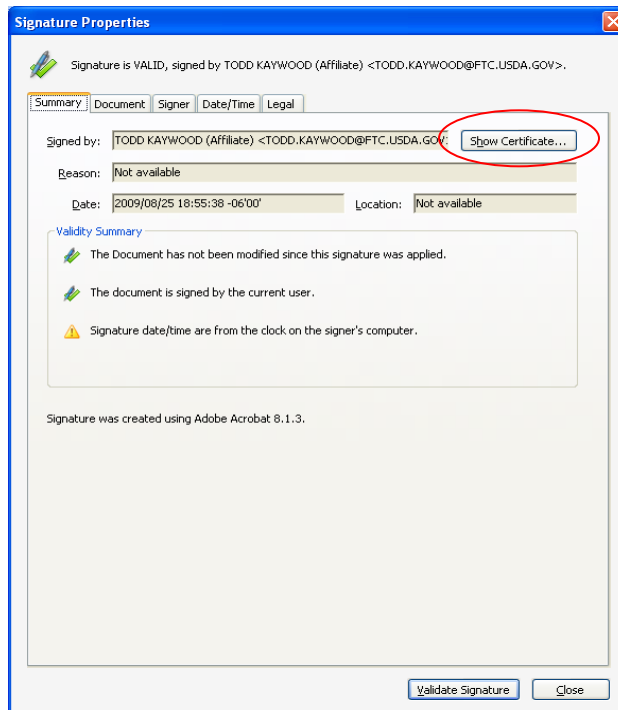
1. Open the file for which you want to verify signatures.
2. You can tell the document has a digital signature because Acrobat automatically displays the Signatures panel. (If Acrobat doesn't automatically open the Signatures panel, click the Signature icon on the left-side toolbar.) The Signatures panel shows the list of the document's digital signatures and the date each was added.



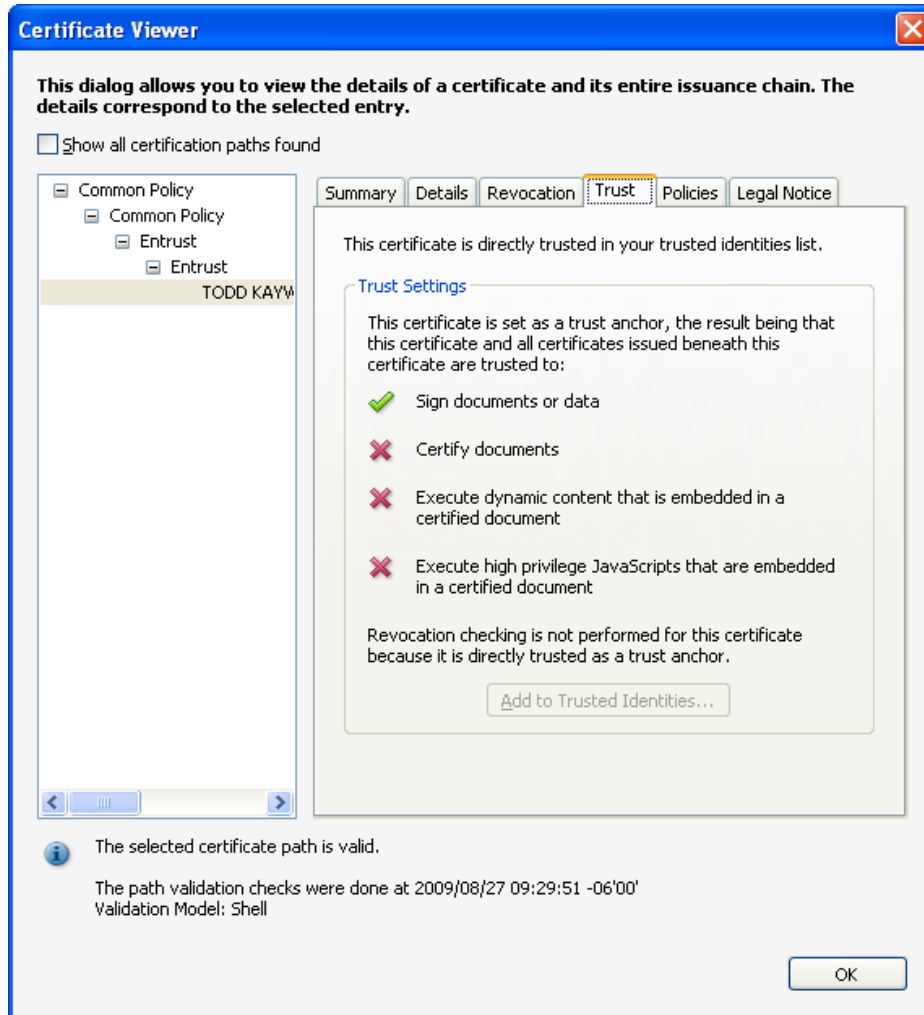
3. A graphic or text also shows where the signature was placed. You can right-click the signature block itself and select "Show Signature Properties" to see details about the signature. Click the **Signature Properties** button.



4. The Signature Properties window shows the name and when the document was signed. If you want to look at the specific certificate details, click the **Show Certificate** button.



5. The Certificate Viewer window shows all the details of the certificate, including the issuance chain, whether or not the certificate is trusted, etc. Click the **OK** button to close the window, then the **Close** button to close the Signature Properties window.



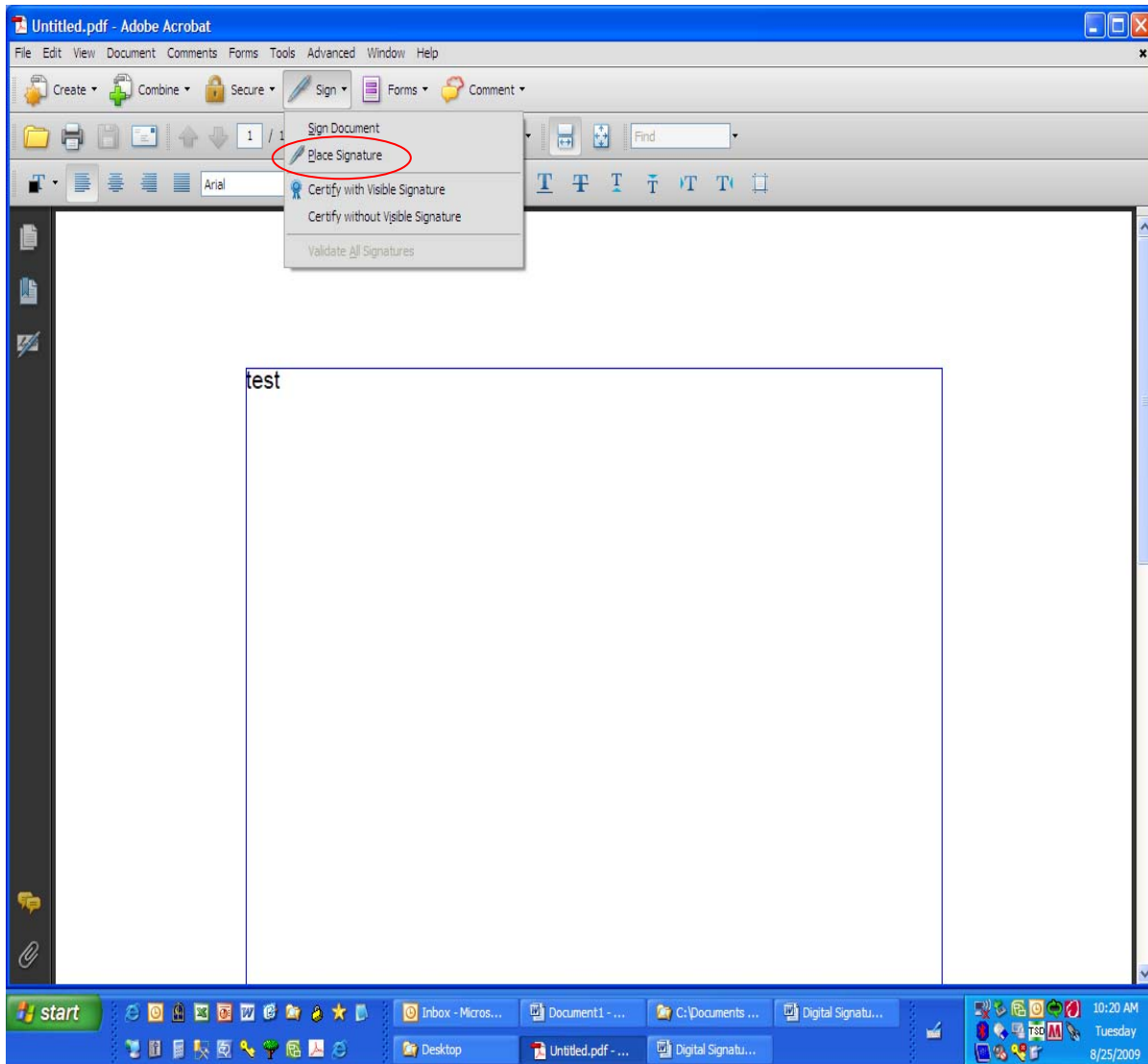
3. Adding a Digital Signature to an Adobe Acrobat 9.x Document

3.1 How to Digitally Sign a Document

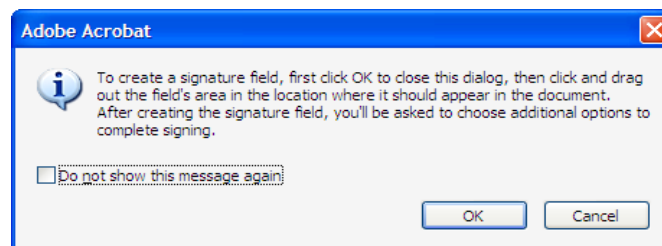
1. Insert your LincPass into the computer's card reader.



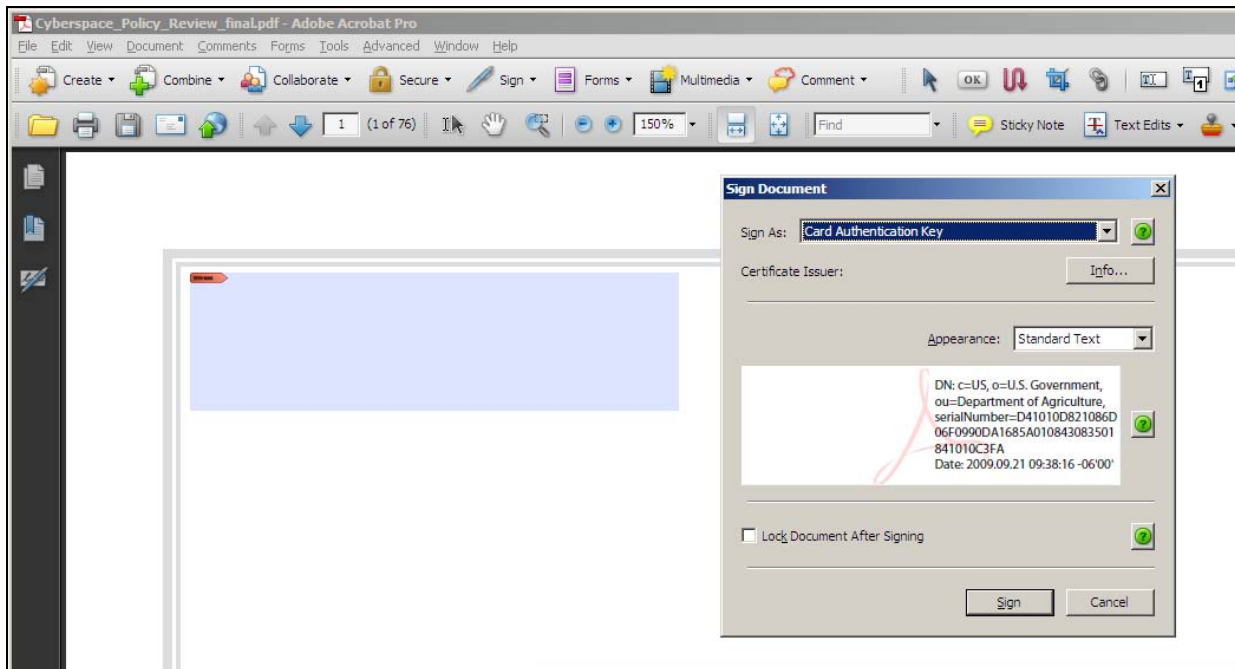
2. Open Adobe Acrobat. Either create a new document or open an existing document you want to sign.
3. From the top menu bar, select Sign, then select "Place Signature."



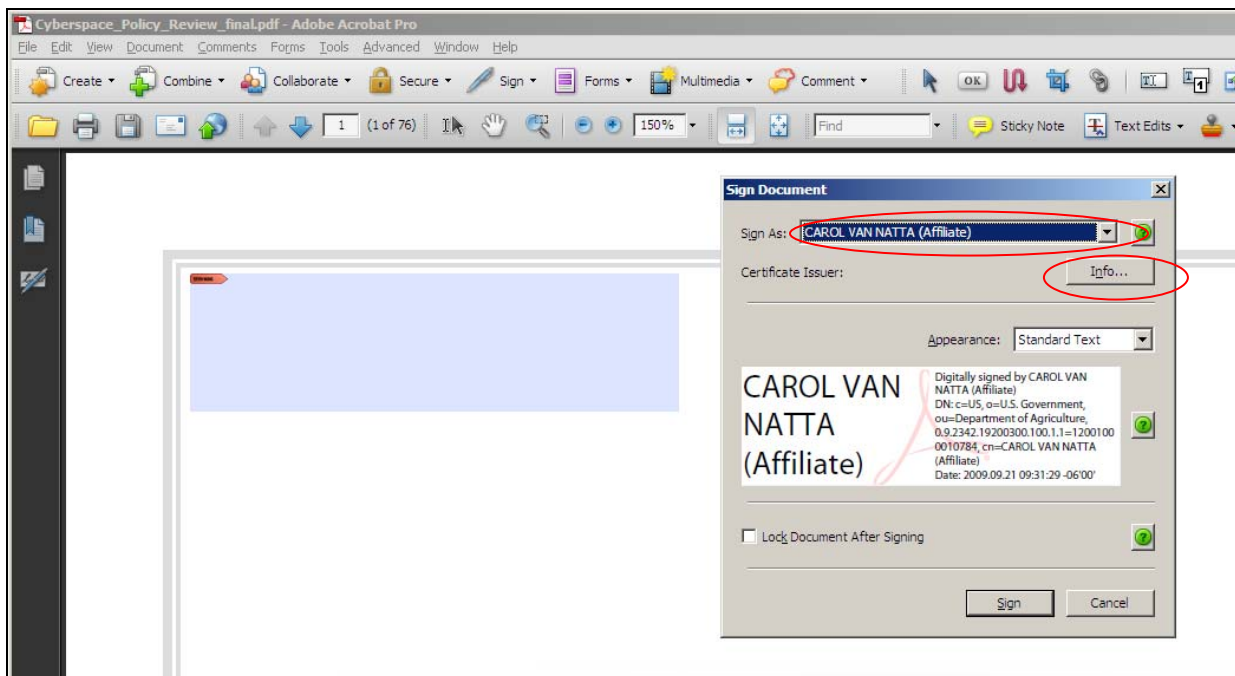
4. Adobe will instruct you to draw an area on the screen where you want to place the signature. Click the **OK** button, then with your mouse, draw a box for the signature. You can set the size of the signature, but it's easier to read if you make it as large as possible. You can place the signature anywhere in your document as well, but the recommended locations are at the beginning or the end of the document.



5. After you have created the signature area, Adobe shows a placeholder for the signature area and displays the Sign Document window.



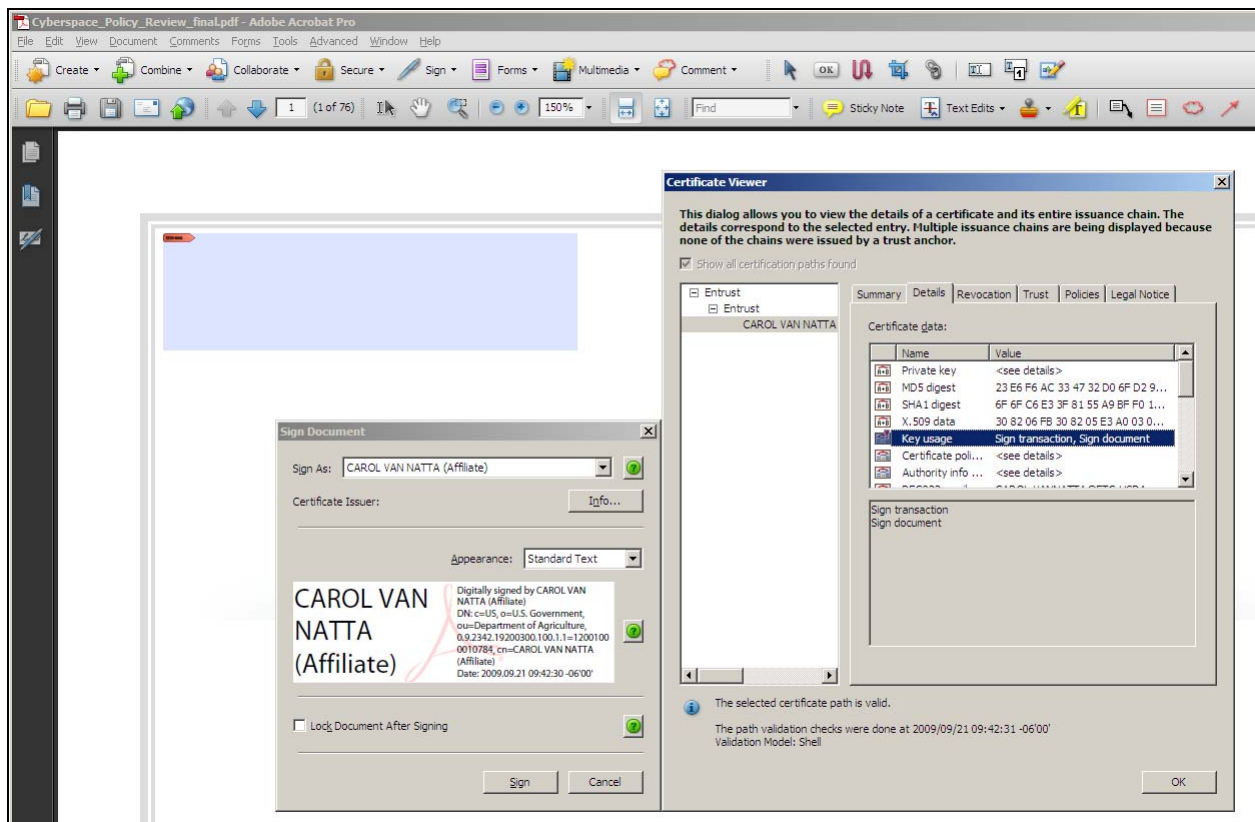
6. From the *Sign As* droplist, select your digital signature key. You will need to view the certificate to confirm it is the correct certificate to use for signing. Select one of the two with your name and then select the **Info** button.



NOTES:

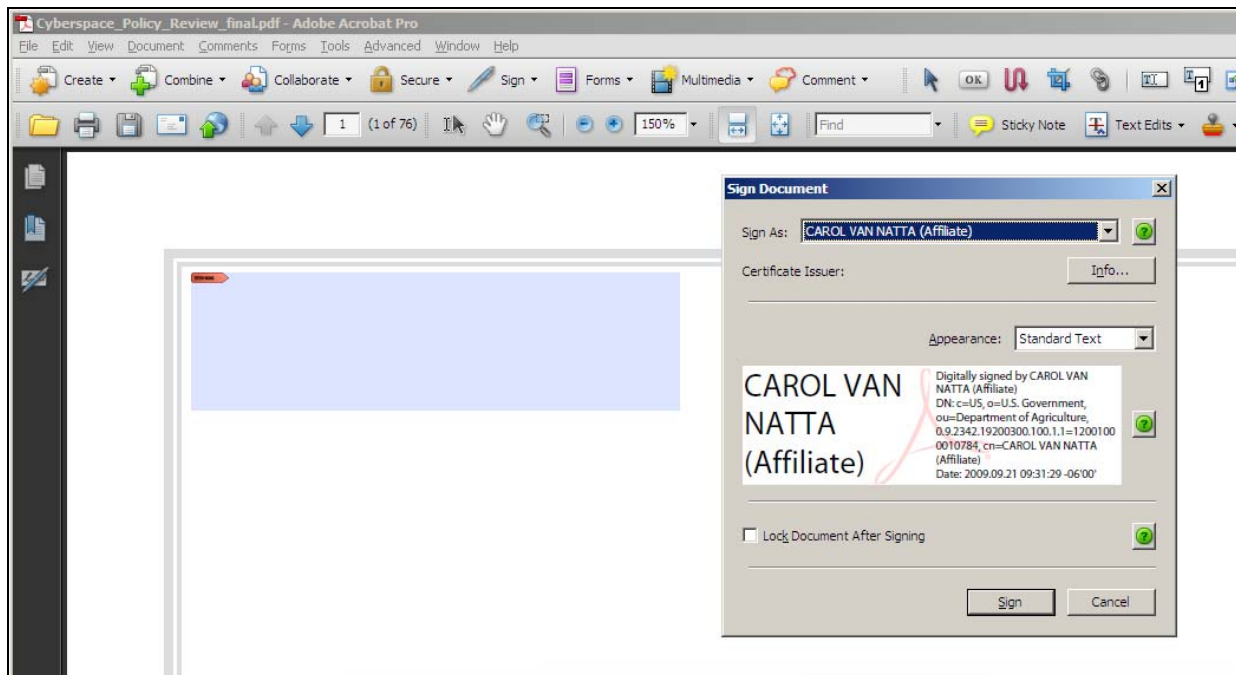
1. If other people with LincPass cards have used your computer, you may see their certificates offered in this list. Only select your personal certificates.
2. If you don't see your certificate keys listed at all, first check that your card is in the reader and wait a minute or two for Acrobat to find it. If your keys still aren't listed, your agency may need to implement the Adobe Technical Modification for Digital Signature. Please ask your system administration or help desk team to work with OCIO-IOA's technical point of contact for help implementing this modification. The technical modification will also save you from having to make this selection each time you want to digitally sign a document.

7. In the Certificate Viewer window, select the Details tab, then in the Certificate data area, scroll down to and highlight the "Key Usage" item. The pane below should say "Sign transaction, Sign document." Click the **OK** button to close the window.

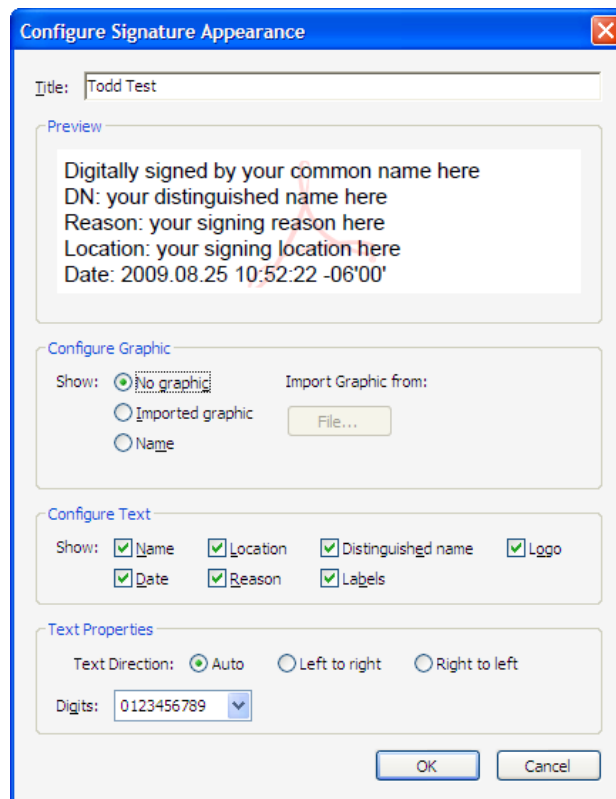


NOTE: If you don't see the correct key usage value, go back to Step 6 and select the other certificate with your name, then repeat steps 6 and 7.

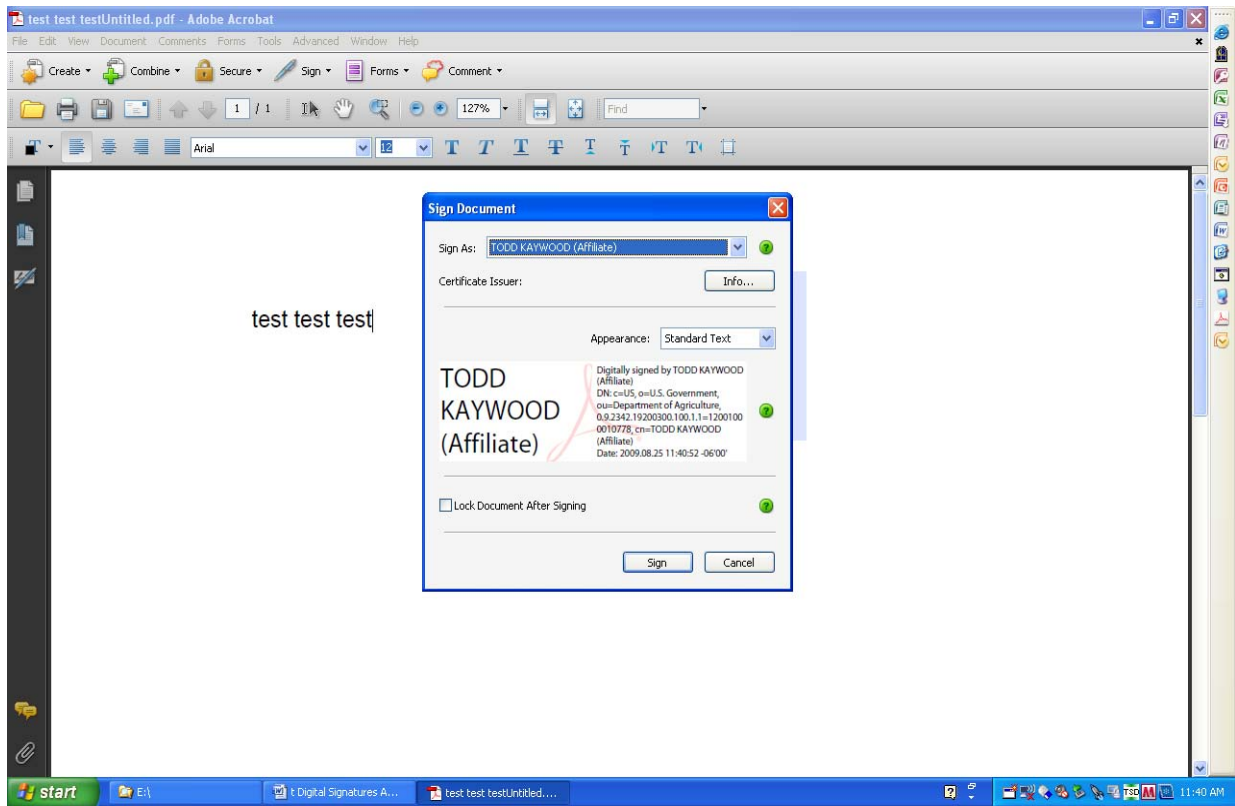
8. You will now be back at the Certify Document screen with your correct certificate selected.



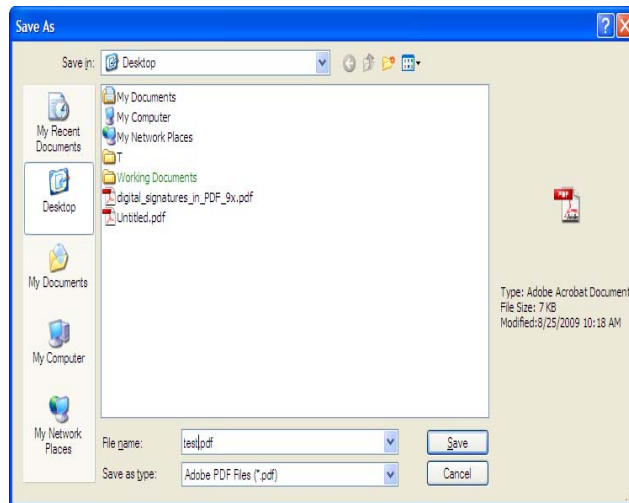
9. **Optional:** You can adjust the appearance of your signature, though it is recommended that you keep the standard text option. If you want to explore the various options, select the Appearance droplist and select "Create New Appearance," to open the Configure Signature Appearance window where you can make changes. If you don't want to make any changes, go to step 10.



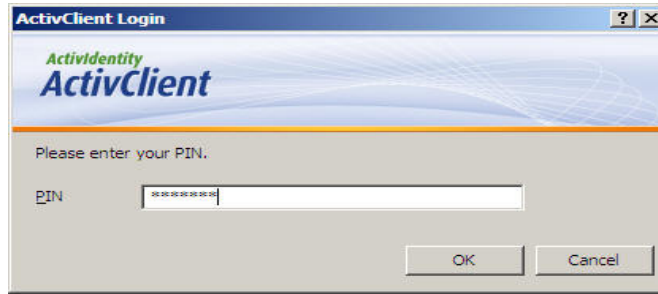
10. In the Sign Document window, click the **Sign** button.



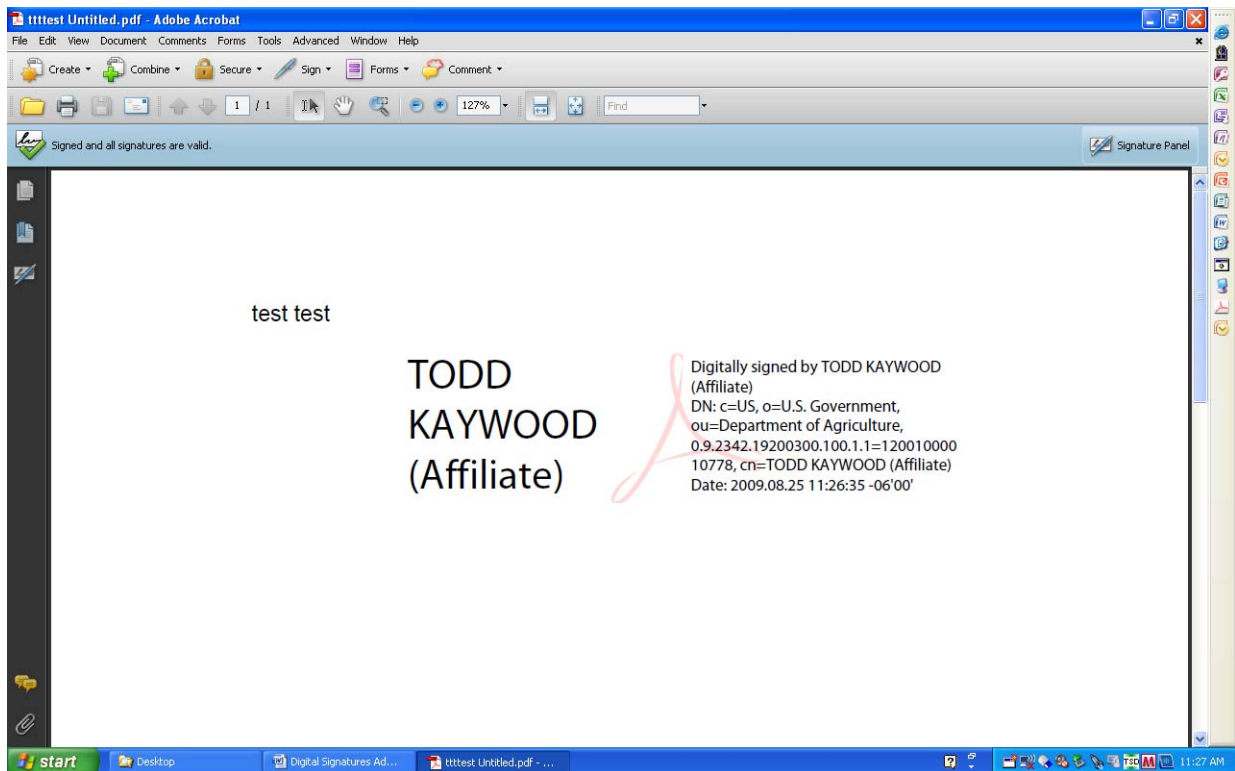
11. When Acrobat prompts you, save the file. If you are working with an existing document, you may want to save it with a new name to distinguish it from the unsigned version of the document.



12. At the ActivClient prompt, enter your LincPass PIN, then press ENTER or click the **OK** button.



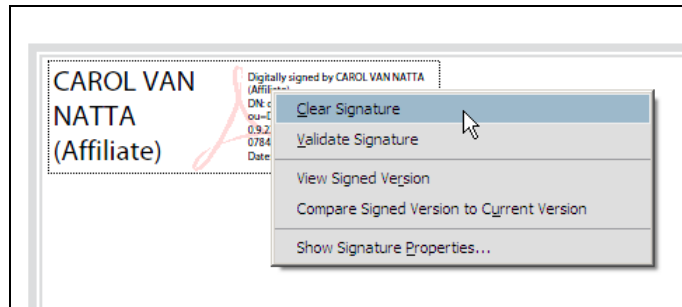
13. Your document is now digitally signed. Close it without making any changes.



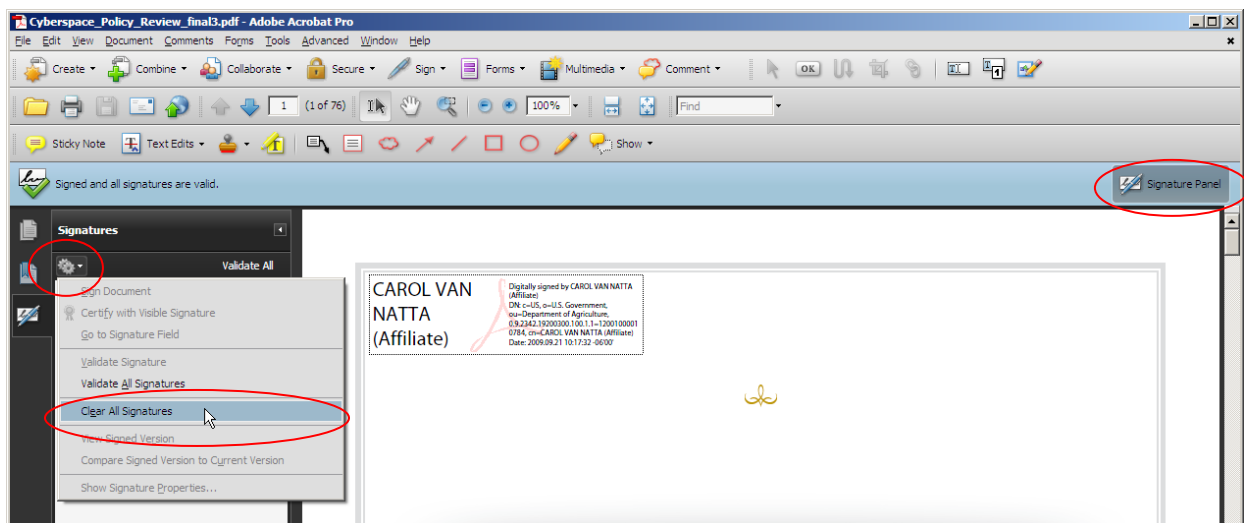
NOTE: Other people can digitally sign the same document by following steps 1-13 in this section. You can have as many people digitally sign the document as needed.

3.2 How to Remove a Digital Signature

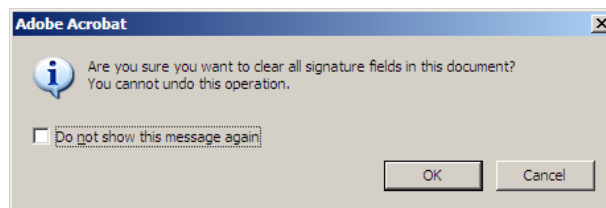
1. Open the file from which you want to remove a digital signature.
2. Find the signature block of the signature you want to remove, and right-click to open the context menu. Select the Clear Signature option to remove this signature.



3. If you want to remove all the signatures at once, open the Signatures panel (click the Signature Panel button in the upper right or the signature icon in the left). Click the Options tab (the gears icon) in the Signatures panel, then select the "Clear All Signature Fields" option.



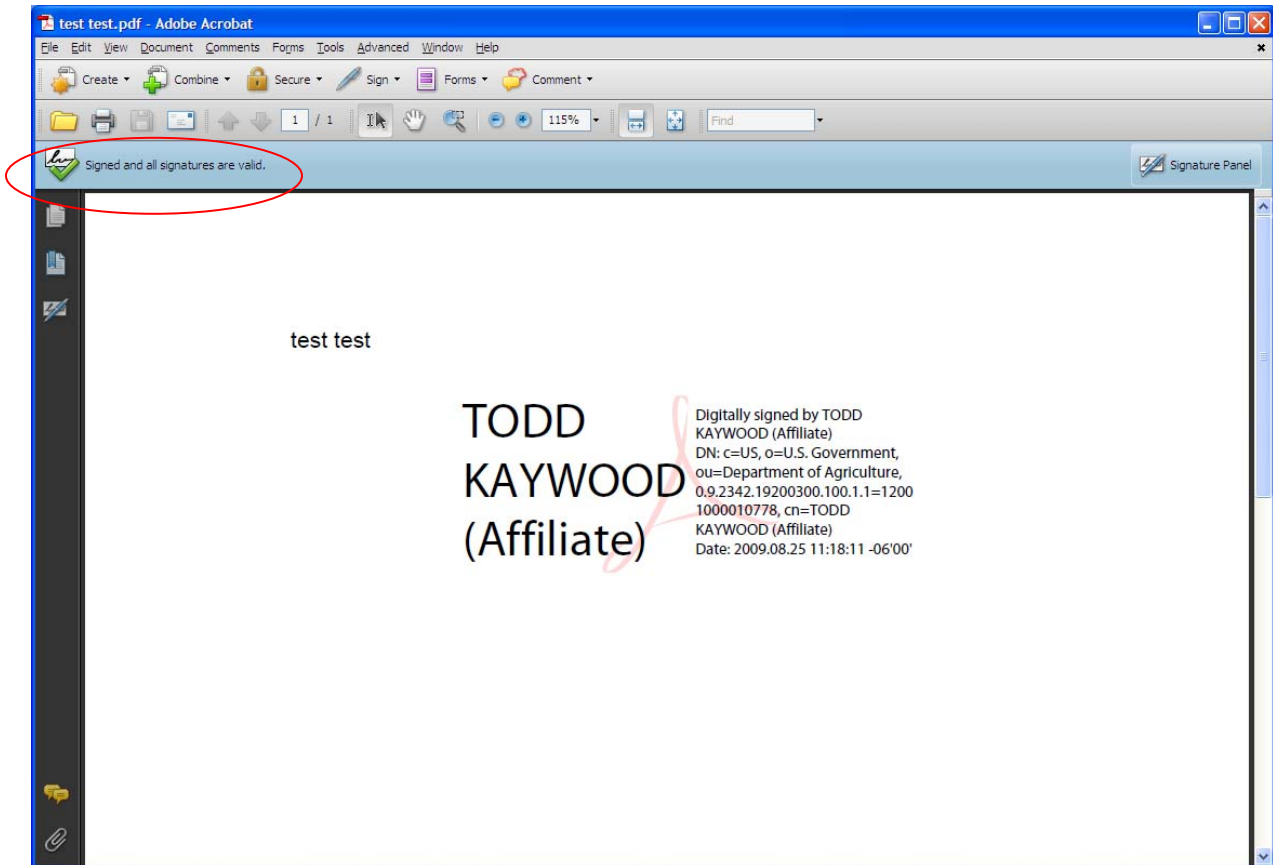
4. Acrobat will warn you that you can't undo this action and ask you to confirm you want to remove the signatures. Click the OK button.



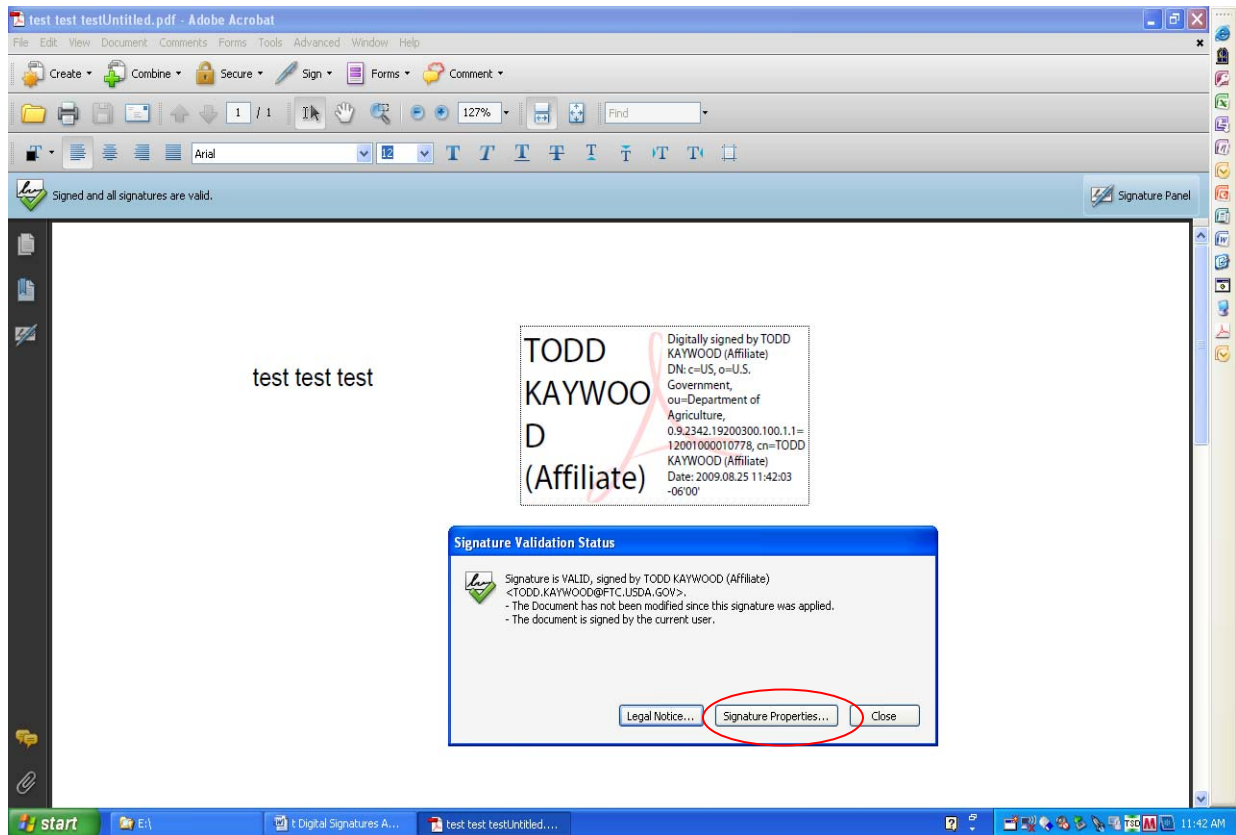
You don't have to save the PDF again, but it won't hurt anything if you do.

3.3 How to Verify a Digital Signature

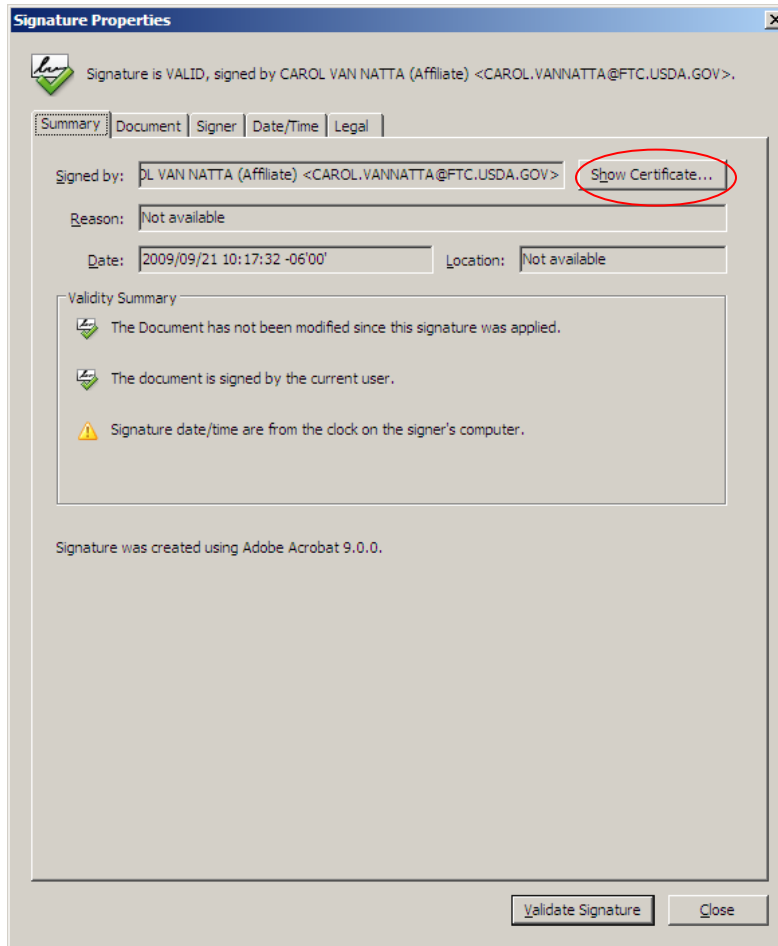
1. Open the file for which you want to verify signatures.
2. You can tell the document has a digital signature because Acrobat displays a message just above the document that the document is signed.



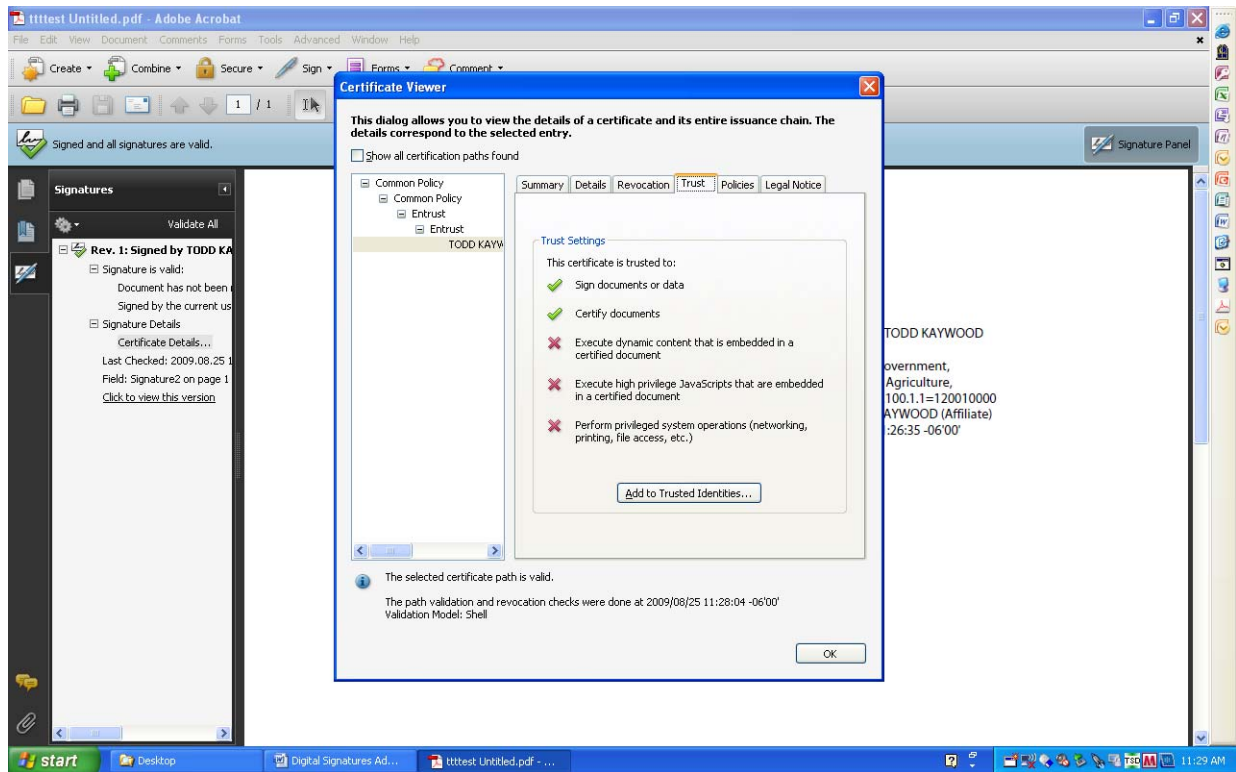
3. A graphic or text also shows where the signature was placed. You can right-click the signature block itself and select "Show Signature Properties" to see details about the signature. Click the **Signature Properties** button.



4. The Signature Properties window shows the name and when the document was signed. If you want to look at the specific certificate details, click the **Show Certificate** button.



- The Certificate Viewer window shows all the details of the certificate, including the issuance chain, whether or not the certificate is trusted, etc. Click the **OK** button to close the window, then the **Close** button to close the Signature Properties window.



4. Help Desk and Troubleshooting for Digital Signature

Problems with digitally signing documents may actually be due to problems with your LincPass. Contact the HSPD-12 help desk for assistance in resolving LincPass issues:

USDA HSPD-12 Help Desk
Toll Free: 1-888-212-9309
Local: 703-245-7888
Email: hspd12@ftc.usda.gov

If you are new to using your LincPass, consider taking the USDA AgLearn course on Two-Factor Authentication for end users (look for course ID "USDA-TwoFactorAuthEndUsers-01").

The Two-Factor Authentication Web site also has information on how to use your LincPass:

<http://hspd12.usda.gov/twofactor.html>

In the middle of the page is a section called "Two-Factor Authentication References," which has instructions on using your LincPass, and will help you confirm you are using your card correctly for digital signature.

If you are still having problems digitally signing documents and you know your LincPass is working correctly, contact your agency's IT help desk or IT system administrator to review your operating system, hardware (computer and card reader), and application software for correct setup and functionality.

You may be able to find answers on digital signature issues at the following vendor Web sites:

Microsoft

Microsoft Digital Signature Support Content:

<http://office.microsoft.com/en-us/outlook/CH010045641033.aspx>

Microsoft General Support:

<http://support.microsoft.com/>

Adobe

Adobe Digital Signature Support Content:

<http://www.adobe.com/security/digsig.html>

Adobe General Support:

<http://www.adobe.com/support/>

5. References

The IOA Digital Signature Web site has information on the project, user guides, technical documents, and policy guidance for digitally signing documents and emails.

IOA Digital Signature Web site:

http://www.ocio.net.usda.gov/wps/portal/ocio/ocioportal/home/ioa/ioa.digital_signature/

Digital Signature User Guides:

http://www.ocio.net.usda.gov/wps/portal/ocio/ocioportal/home/ioa/ioa.digital_signature/

- Digital Signatures Microsoft Office – 2003 (*this document*)
- Digital Signatures Microsoft Office – 2007
- Digital Signatures Microsoft Outlook– 2003 and 2007
- Digital Signatures Adobe Acrobat 8 & 9

Technical Configuration Guide Change

http://www.ocio.net.usda.gov/wps/portal/ocio/ocioportal/home/ioa/ioa.digital_signature/

- Digital Signatures Adobe Configuration Change To Registry setting for Certificates

Policy Guidance

http://www.ocio.net.usda.gov/wps/portal/ocio/ocioportal/home/ioa/ioa.digital_signature/

- OCIO I&OA Digital Signatures Policy Guidance

Vendor Web sites have information on how to apply digital signatures in their products:

Microsoft Office

Location: Microsoft Support Site

<http://www.microsoft.com/downloads/details.aspx?FamilyId=79d06e72-4b45-4669-9eac-0eca5821e8ff&displaylang=en>

Microsoft Outlook

Location: Microsoft Support Site

<http://www.microsoft.com/downloads/details.aspx?FamilyId=CC37CC1E-028D-4D30-9093-96CC6513ECA1&displaylang=en>

Adobe Acrobat 8 & 9

Location: Adobe support site

<http://learn.adobe.com/wiki/display/security/Document+Library>
<http://www.adobe.com/security/digsig.html>

USDA Web sites have general information on the issuance, activation, and use of the LincPass card:

HSPD12

<http://hspd12.usda.gov/index.html>
<http://hspd12.usda.gov/faq.html>

Two-Factor Authentication

<http://hspd12.usda.gov/twofactor.html>
