

OFFICE OF THE CHIEF INFORMATION OFFICER
INNOVATIONS & OPERATIONAL ARCHITECTURE

User Guide for Digital Signatures in Microsoft Office 2007 (Word, Excel, PowerPoint)

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 Microsoft Office – 2007.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 a Word, Excel, or PowerPoint 2007 Document	6
2.1 How to Digitally Sign an Office 2007 Document	6
2.2 How to Remove a Digital Signature from an Office 2007 Document.....	10
2.3 How to Verify a Signature is Valid	11
3. Help Desk and Troubleshooting for Digital Signature	12
4. References	12

1. Introduction

This document provides instructions on how to add digital signatures to Microsoft Office 2007 (Word, Excel, and PowerPoint) 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 Microsoft Office 2007 installed.

NOTE: These instructions are based on the FDCC-approved installation of Microsoft Office 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 Outlook 2003 and 2007 (for sending digitally signed emails)
- Microsoft Office 2003
- Adobe Acrobat versions 8 and 9

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

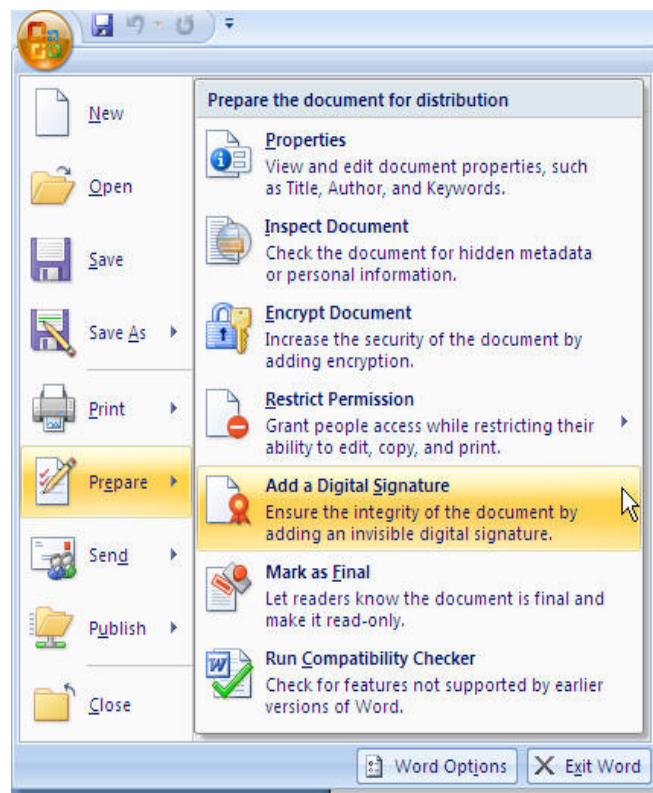
- **PIV card:** FIPS 201-compliant personal identity verification (PIV) card.
- **LincPass:** USDA's name for the PIV cards it issues to employees, contractors, partners, affiliates, et al.
- **HSPD-12:** Homeland Security Presidential Directive 12, signed 27 August 2004. HSPD-12 requires all federal 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 a Word, Excel, or PowerPoint 2007 Document

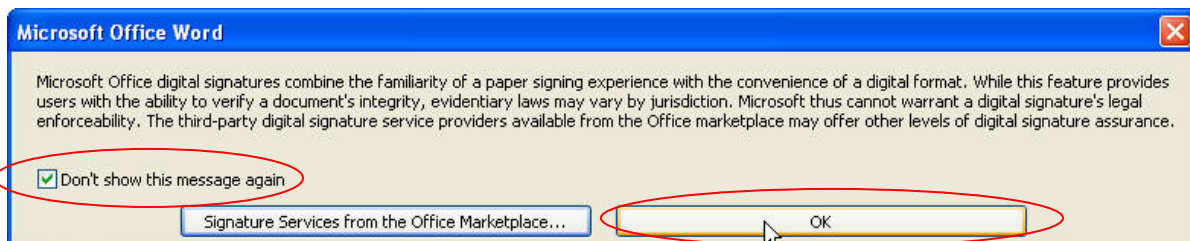
In the following user guide steps the process for digital signature covers Word, Excel, and PowerPoint. Though the programs are different, the steps, menu choices, and windows are the same in all three. In the following subsections, an Office 2007 document refers to a Word, Excel, or PowerPoint document.

2.1 How to Digitally Sign an Office 2007 Document

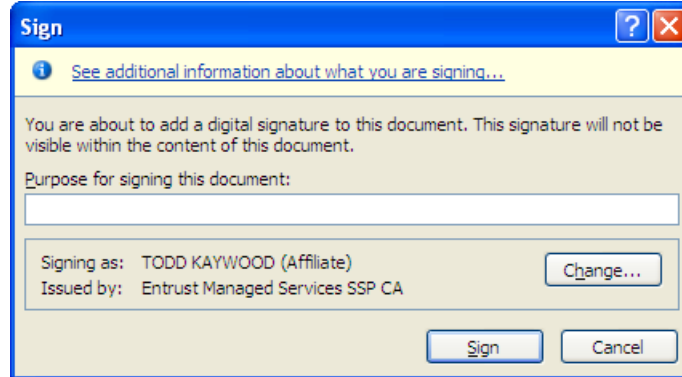
1. Insert your LincPass into the computer's card reader.
2. From the main menu icon, select **Prepare**, then **Add a Digital Signature**.



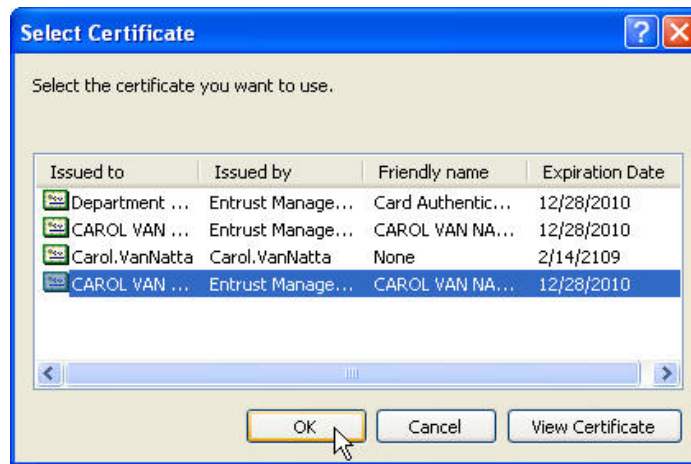
3. If this is the first time you've selected a certificate for digital signing, Microsoft offers to help you set one up. Since your LincPass already has certificates, click the **OK** button. (To avoid seeing this message each time, check the "Don't show this message again" option.)



4. In the **Sign** window, complete the optional “Purpose for signing this document” field, then click the **Change** button to confirm you have the correct Certificate selected.

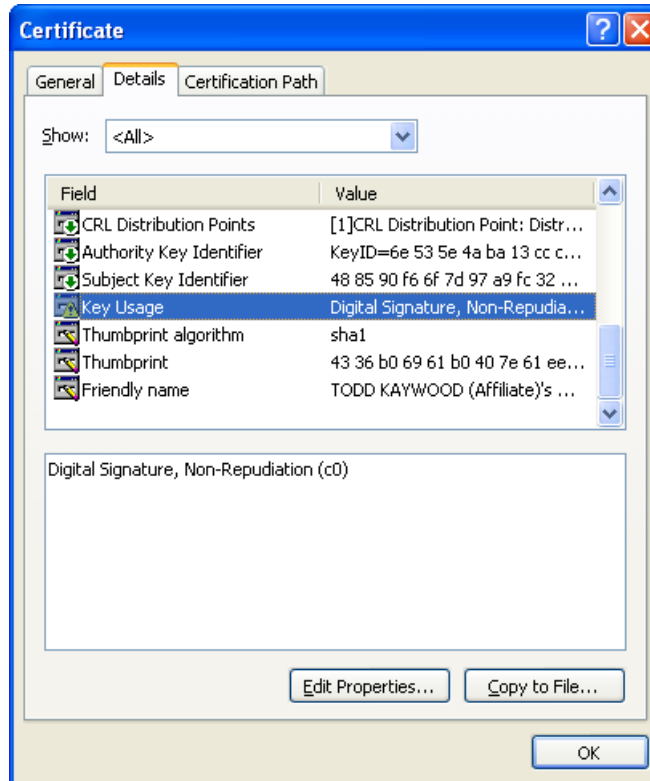


5. Select the certificate you want to use by highlighting it. (The next step will help you determine which is the correct certificate to select.)

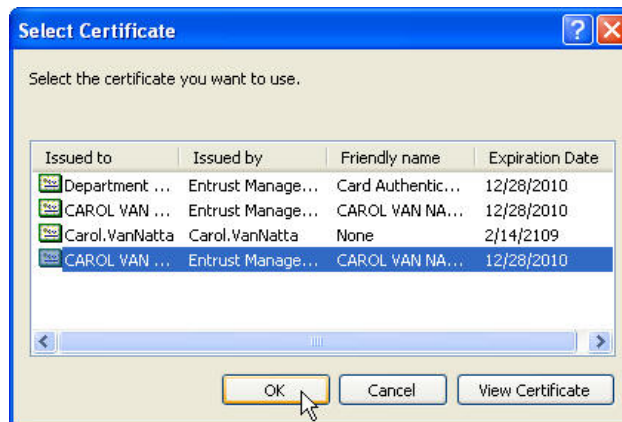


- Click the **View Certificate** button. The *General* tab lists the information about the certificate. Click the *Details* tab. Scroll down in the list of fields and values to select the “Key Usage” field. In the field below, it should say “Digital Signature, Non-Repudiation (c0)”. Click the **OK** button to close the window.

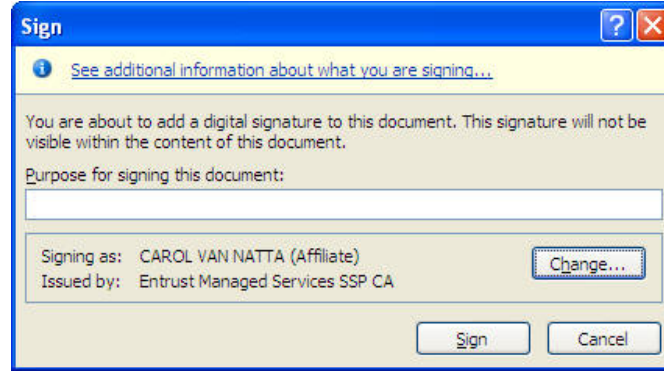
NOTE: If the “Key Usage” field only says “Digital Signature” or something else, go back to step 5 and select one of the other certificates and use the **View Certificate** button to verify it’s the one you want.



- Back on the list of certificates, with the correct certificate highlighted, click the **OK** button.

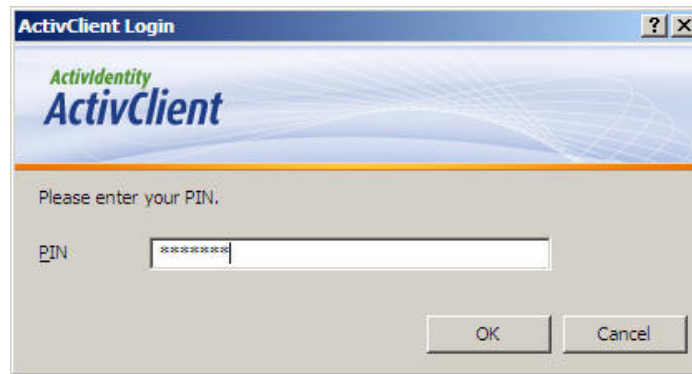


8. Back on the **Sign** window, Click the **Sign** button.



NOTE: After you select the certificate the first time, Office 2007 will remember this certificate choice. The next time you want to digitally sign a document, you won't have to repeat the selection process – you'll jump from step 4 to step 8 in this sequence.

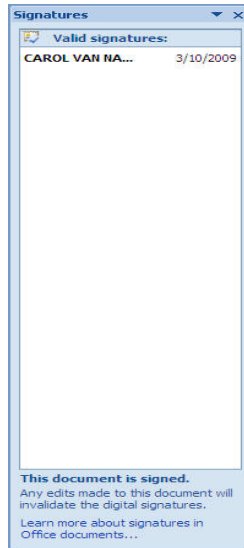
9. At the ActivClient prompt, enter your LincPass PIN, then press ENTER or click the **OK** button.



10. After the Certificate is validated, you will receive a successful signature message. Click the OK button.



11. Once the signature has been successfully applied, Office 2007 automatically opens a *Signatures* window on the right side of screen showing the valid signature(s).



12. The Word, Excel, or PowerPoint file is now digitally signed by you. Close the file without making any changes (or the digital signature will be lost).

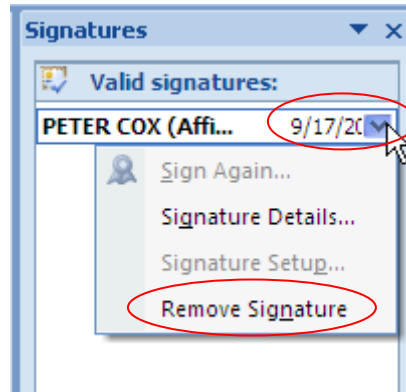
NOTE: More than one person can digitally sign a document, as long as the content of the document isn't changed. After the first signature is applied and the file closed, the second person can follow steps 1-12 above to apply a second signature. This can be repeated for as many signatures as are needed.

2.2 How to Remove a Digital Signature from an Office 2007 Document

If you want to remove all digital signatures from a document, the simplest way is to make a minor change to the document (e.g., add a space), then save the document. When Office 2007 warns you that all signatures will be lost, click the **Yes** button to continue the save operation.

If you want to remove one or more digital signatures from the document without changing the document contents, follow these steps:

1. From the *Signatures* window on the right side of the screen, select the signature you want to remove, then click the right-side drop arrow.




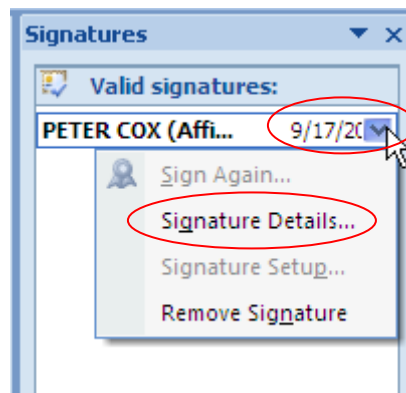
2. Select the "Remove Signature" option. Click OK to confirm you want to remove the signature.

That digital signature has now been removed from the Office 2007 document.

2.3 How to Verify a Signature is Valid

1. Open the file for which you want to verify signatures.
2. You can tell the document has a digital signature because the *Signatures* window automatically opens when you open the document. The window lists valid signatures and the date the signature was added. If you want to see signature details, highlight and right-click the digital signature, then select "Signature Details" to view the certificate behind it.

 **NOTE:** If the window doesn't open automatically, click the small red certificate icon in the bottom status information bar.



3. 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/>

4. 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/ia/ia.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/ia/ia.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/ia/ia.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>

-- -- --