

CC-2020-005

April 1, 2020

Procedures Related to Electronic
Clearance and Digital Signatures for
Office of Chief Counsel Documents and

Subject: Regulations

Cancel Date: Until Further Notice

This notice announces changes to procedures for clearing and signing Office of Chief Counsel documents and regulations.

Electronic Clearance of Office of Chief Counsel Documents

Effective immediately, any Office of Chief Counsel document may be cleared electronically. Where a physical document or file previously would have been used to clear a document, the same document may be submitted to the approving official electronically via email. The subject line of the email should reflect that a document is being submitted for clearance. The file name of the document being cleared should indicate the type of document being cleared, the subject (e.g., CASE-MIS number and title), and the date of the draft document. If comments are provided on or revisions are made to the document, the file name of the document that is returned to the drafting attorney should reflect who made the comments or revisions and the date of the comments or revisions.

Official agency records for documents will continue to be maintained in paper form in accordance with agency recordkeeping requirements, unless otherwise provided for in the Chief Counsel Record Control Schedules. See Document 12990, Record Control Schedules, and CCDM Part 30.9. Compliance with this requirement will necessitate printing documents that have been digitally signed and adding them to the official agency record before the file is closed. All paper files still must be maintained in accordance with the requirements in CCDM Part 30.9, which include printing all significant drafts.

Specific Information for Electronic Clearance of Regulations and Internal Revenue Bulletin Guidance

Documents that may be cleared electronically include regulations and other guidance published in the Internal Revenue Bulletin (IRB). Regulations or IRB guidance should be circulated for clearance in an email that contains, as attachments, all of the documents that would have been included in a physical clearance folder. See CCDM

Distribute to:	Tax Litigation staff	Tax Litigation staff & Support personnel
	X All Personnel	Electronic Reading Room
Filename:	CC-2020-005	File copy in: CC:FM:PFD

32.1.6.8.1. and CCDM 32.2.7.2. If those reviewing the document provide comments or make revisions, the file name for the document that is returned to the drafting attorney should reflect who made the comments or revisions and the date of the comments or revisions. Once those reviewing the document are ready to clear it, they should reply to the clearance email stating their approval. The drafting attorney then should type the name of the reviewer, the reviewer's office, and the date of approval into the pink clearance sheet or the Background Information Note (BIN) after each approval is received. Alternatively, the pink clearance sheet or the BIN may be digitally signed to document approval.

Use of Digital Signatures on Office of Chief Counsel Documents

Effective immediately, digital signatures may be used to sign any Office of Chief Counsel document, including but not limited to: published guidance, Chief Counsel legal advice, letters to the Department of Justice, Action on Decisions (AODs), and Private Letter Rulings (PLRs). Methods of digital signatures include:

- Converting a document to a PDF and adding a signature in Adobe Acrobat;
- Scanning an image of a signature and adding to the document; or
- Adding “/s/” and the person's name to the text of the document and then locking the document as provided in Exhibit 1.

Procedure to Obtain Digital Signatures on Regulations

Regulations may be signed digitally in accordance with Federal Register requirements, which are attached as Exhibit 1. The Office of the Federal Register requires that documents submitted for publication in the Federal Register be signed in Microsoft Word by adding an invisible digital signature. This process prevents the text of the document from being revised after the invisible digital signature is applied. Consequently, signing the document must be the last act performed before the document is submitted to the Federal Register for publication.

A document is ready for digital signature once the regulation has been approved for publication by the Office of Chief Counsel, the Office of the Deputy Commissioner, Services and Enforcement (DCSE), and the Treasury Department and prepared for submission by the assigned Federal Register Liaison (FRL) in the Publications and Regulations Branch of the Legal Processing Division of Procedure and Administration. At that point, no more changes can be made to the document.

To digitally sign a Microsoft Word document, the following steps must be performed in the following order:

1. After the document is approved by Treasury, the document, pink clearance sheet, and record of Treasury approval is e-mailed by the Associate Office to the assigned FRL to prepare the document for signature.

2. After preparing the document for signature, the FRL emails the final document to the assigned attorneys in the Associate Office that is responsible for the regulation.
3. The Associate Office emails the document to the Senior Advisor to the DCSE. The title of the e-mail must begin with the following: "FOR ELECTRONIC APPROVAL/DIGITAL SIGNATURE." The Senior Advisor to the DCSE will facilitate obtaining the digital signature of the DCSE or the person acting in that capacity. The document must be digitally signed in accordance with the Federal Register requirements. The Federal Register steps for digitally signing documents for submission to Office of Federal Register are attached as Exhibit 1.
4. The Senior Advisor to the DCSE returns the digitally signed regulation to the Associate Office responsible for the regulation.
5. For Treasury Decisions only, the Associate Office emails the document that was digitally signed by the DCSE to the Attorney-Advisor in the Treasury Department who is responsible for the regulation. The Attorney-Advisor obtains the digital signature of the Assistant Secretary for Tax Policy, or the person acting in that capacity, in accordance with Exhibit 1. The Attorney-Advisor then emails the document signed by the Assistant Secretary for Tax Policy (and the DCSE) back to the responsible Associate Office.
6. The Associate Office emails the final digitally signed document to the assigned FRL, who will transmit the document to the Federal Register.

If you have any questions about these procedures, please contact Emily M. Lesniak at Emily.M.Lesniak@irs.counsel.treas.gov or 202-317-5409 in the Office of the Associate Chief Counsel (Procedure & Administration).

_____/s/
Kathryn A. Zuba
Associate Chief Counsel
(Procedure & Administration)

Exhibit 1

Digitally Signing Documents for Submission to Office of the Federal Register

Publish Date: July 17, 2018

The digital signatory of a document **MUST** be the same person whose name is typed in the signature block. The names must match exactly or meet the accepted standards listed in the DDH, Ch. 1. To verify the name as applied to the digital certificate, follow the instructions below in the [View Signature Certificate in MS Word](#) section.

Using the native Microsoft (MS) Word signing capability applies your Public Key Infrastructure (PKI) certificate to the document, guaranteeing the authenticity of the signer and the document. Once applied, your document is protected and cannot be edited without removing the digital signature. The MS Word signing process saves the signed document *under the same filename!*

Use MS Word 2010 or later. Only submit “.docx” file types. Older versions of MS Word have no standard method to validate digital signatures. The old file type “.doc” is not compatible with OFR’s digital validation process and is not accepted in the web portal.

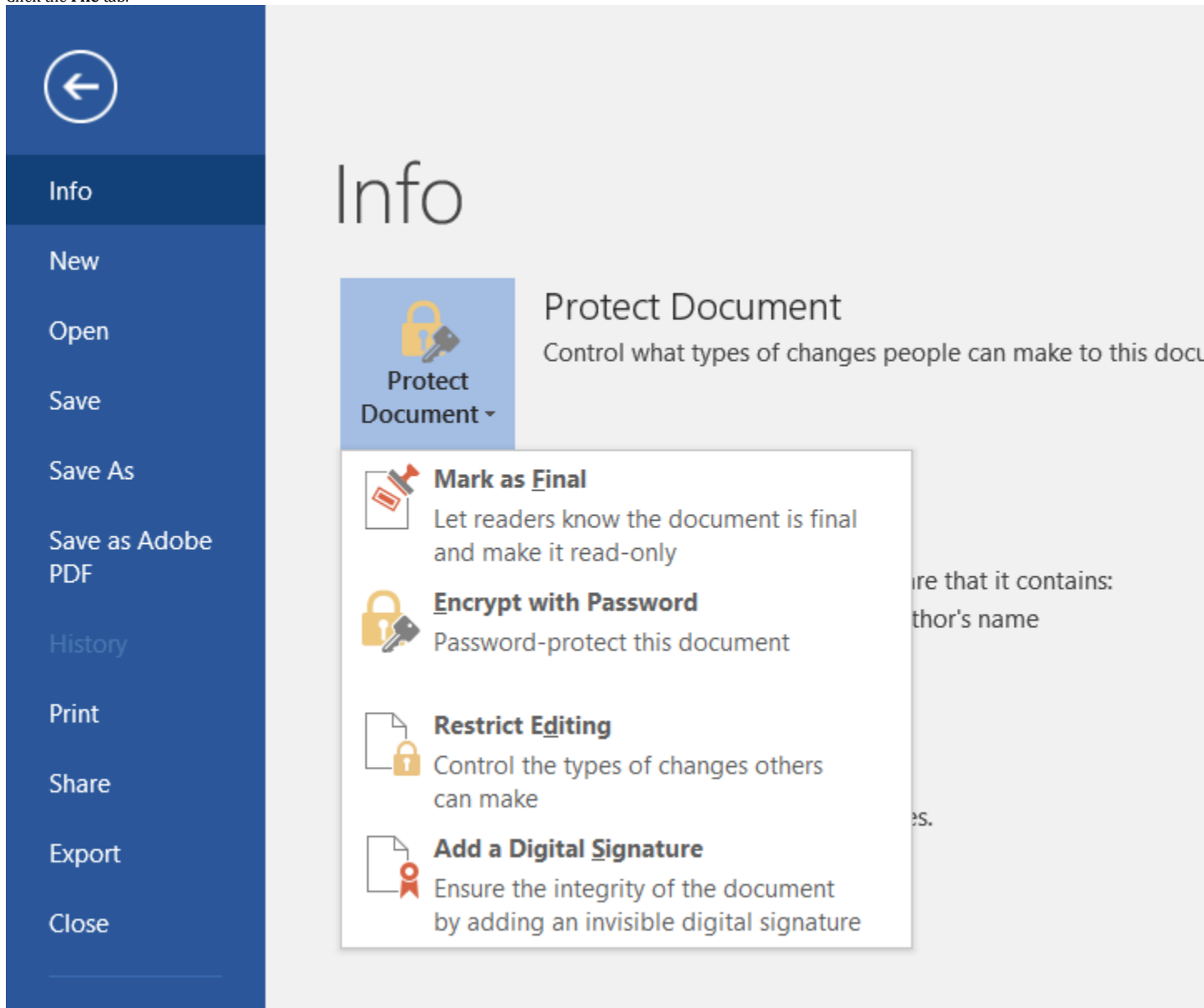
Do **NOT** use the *Insert Signature* function (under the **INSERT** tab in the **Word** ribbon). Follow the instructions below to sign the document invisibly as this is the format OFR will accept.

Add Invisible Digital Signatures in MS Word

IMPORTANT: The following instructions apply to MS Word 2013. The signing process for other MS Word versions (e.g., 2010, 2016, Office 365) may vary somewhat. If you have trouble with the signing process, contact OFR at ofrtechgroup@gpo.gov or (202) 741-6020 or your IT support.

1. Open your MS Word document in Word. Any changes must be saved before signing.
2. If you have a purchased PKI credential installed on your computer, proceed to Step 3. Otherwise, insert your Federal Government-issued Personal Identity Verification (PIV) card into your card reader.

3. Click the **File** tab.

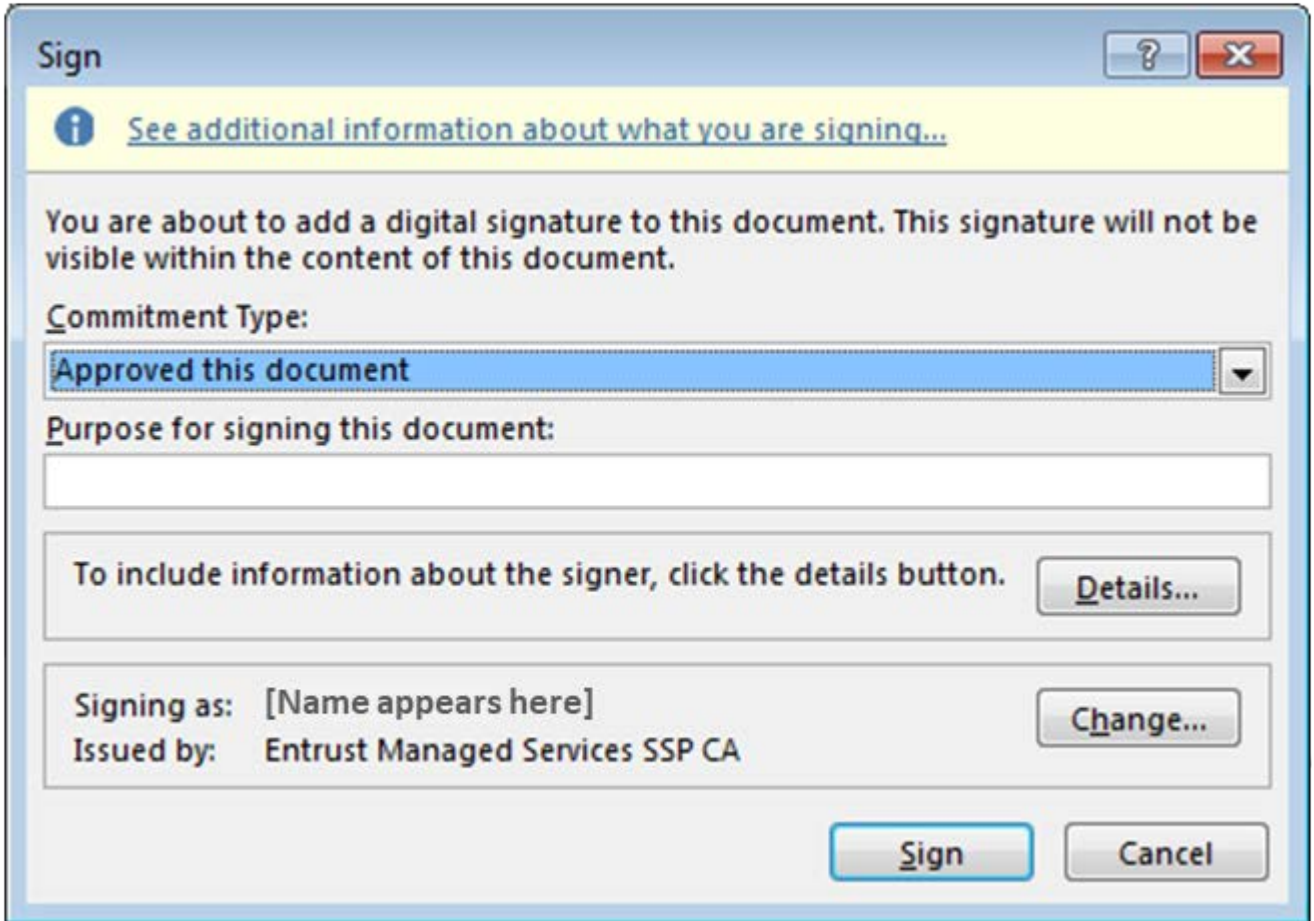


4. Click **Info**.

5. Click **Protect Document**.

6. Click **Add a Digital Signature**.

7. In the **Sign** dialog box:

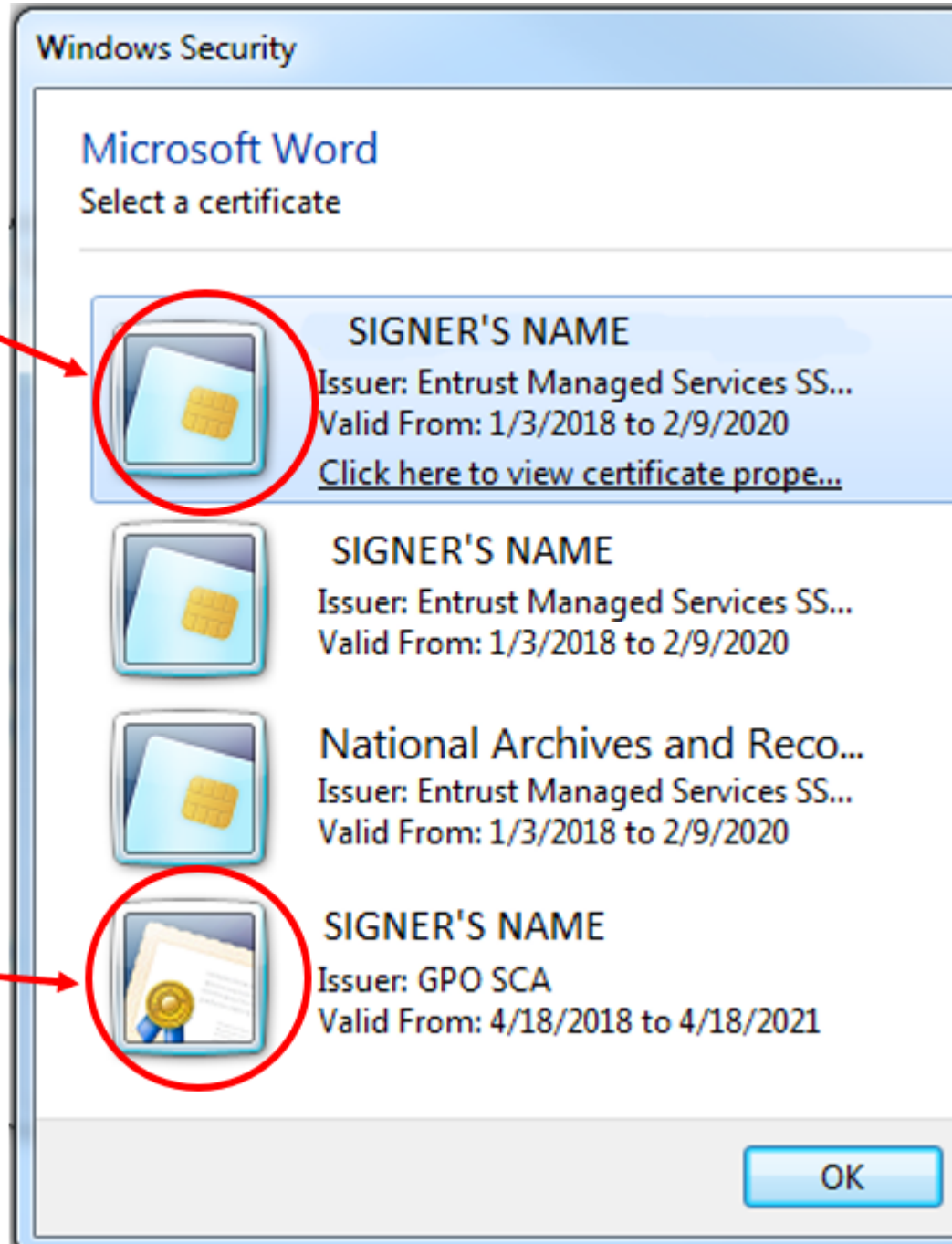


8. Select a **Commitment Type** from the pull-down menu.
9. In the **Purpose for signing this document**, type the purpose or leave blank.
10. To ensure the correct certificate is used, click the **Change** button.

11. In the Certification Selection box, there may be multiple certificates. Select the first **unexpired** certificate with your name; then *Click here to view the certificate properties*.

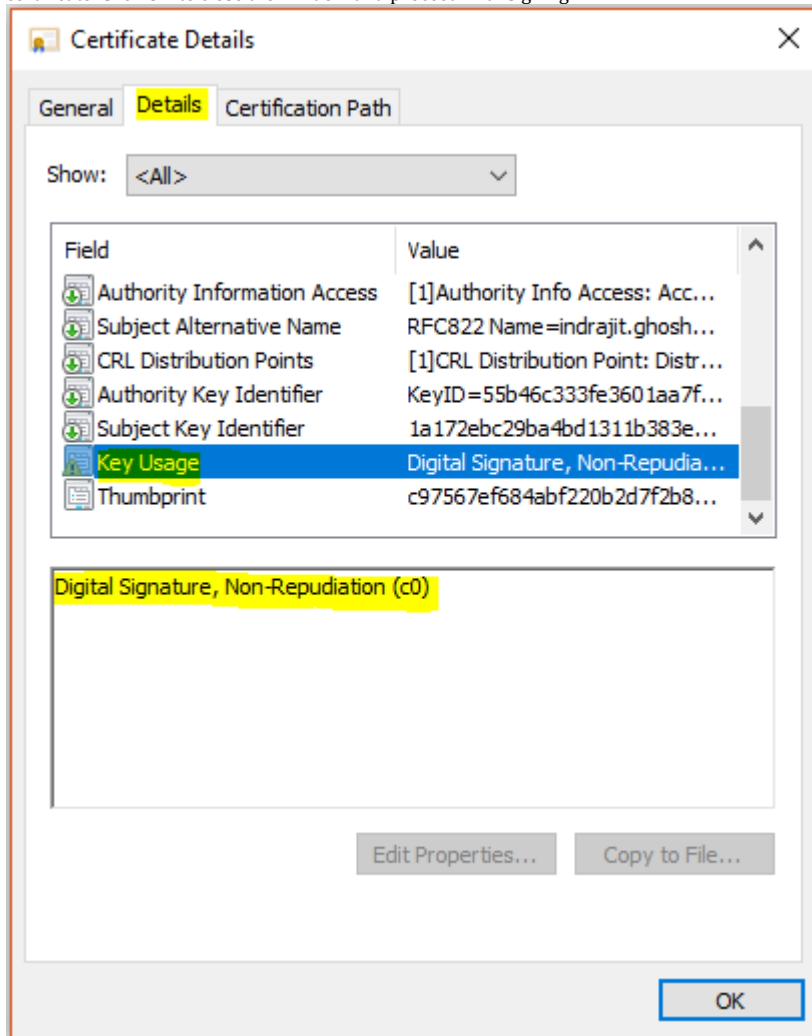
Indicates
PIV certificate

Indicates
purchased
certificate



12. The **Certificate Details** box appears. Go to the *Details* tab and scroll down to *Key Usage*. Single-click on it. The lower text box should now display "Digital Signature, Non-Repudiation" (for PIV card certificate) or "Digital Signature" (for a purchased certificate). If it does, then this is the right

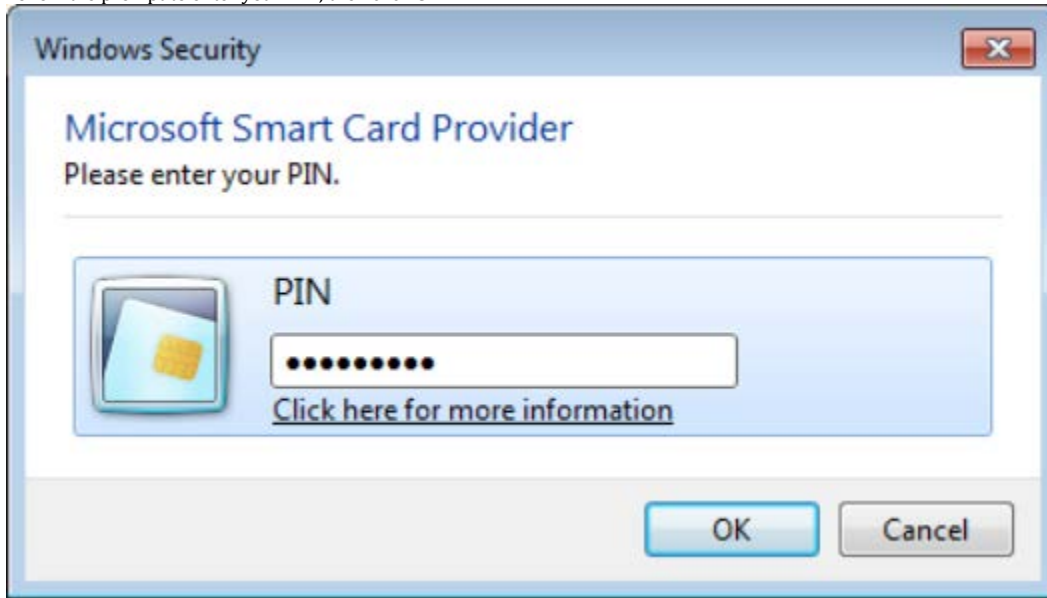
certificate. Click **OK** to close the window and proceed with signing.



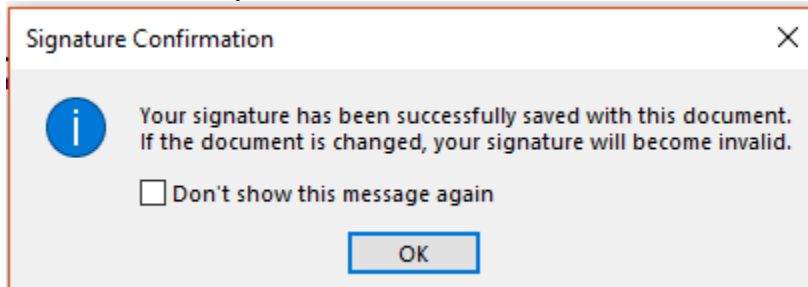
13. If this is the wrong certificate, click **OK**. Then select another certificate and repeat these steps until you find the correct certificate.

14. Click **Sign**.

15. Follow the prompt to enter your **PIN**; then click **OK**.



16. If the digital signature certificate and PIN are valid, the document is signed and automatically saved *under the same filename!* This is the file you submit to OFR via the web portal.



If you are signing multiple documents, leave MS Word open and your PIV card inserted to sign without having to re-enter your PIN for each file.

For multiple-signatory documents (e.g., dual-agency submissions), the first signer forwards the signed document to the next signer, who repeats the signing process on the *already-signed file*. See the [Multiple Digital Signatories in MS Word](#) section below. All digital signatories must have their names and titles typed into a separate signature block in the signature block area of the document.

A digital signature can be removed if necessary. This might be handy if last-minute changes are needed or if a different signatory is desired. Remember that the document will have to be re-signed prior to submission to OFR. See [Remove Invisible Digital Signatures in MS Word](#) below.

Multiple Digital Signatories in MS Word

Multi-agency digital submissions are not only possible but recommended. Exactly like paper-and-disk submissions, if multiple agencies are submitting a document for publication, OFR receives only one document, signed by all agencies. For example, if six agencies are jointly issuing a rule, OFR does NOT get six submissions of the same rule. Regardless of the method of submission, the legal requirements are the same; i.e., representatives from all issuing agencies must sign the document (DDH, 1.6). If one or more of the agencies are unable or unwilling to digitally sign, the document must be submitted via the conventional paper-and-disk procedure (DDH).

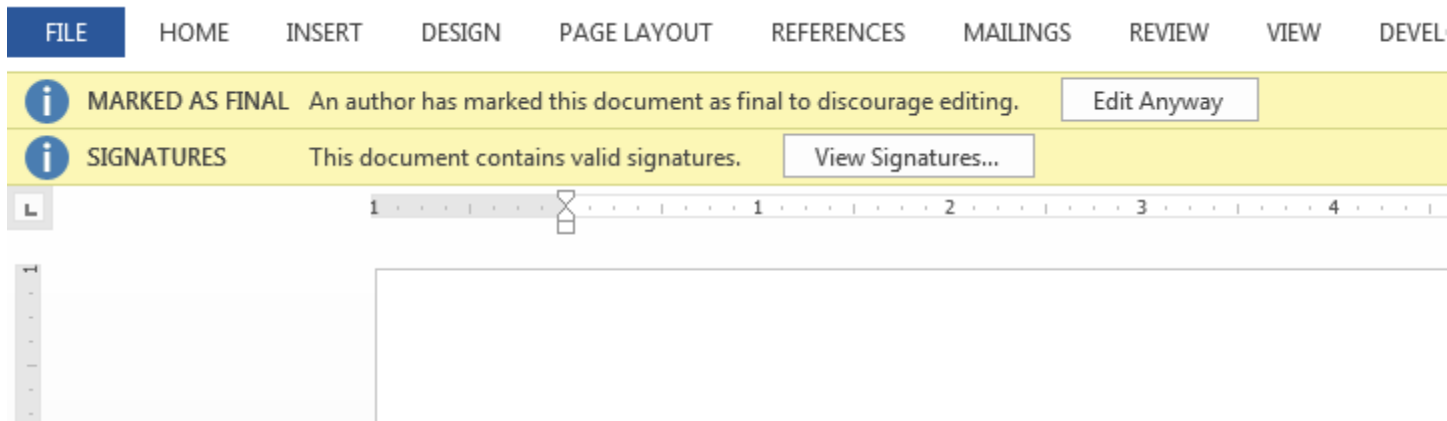
One of the issuing agencies should serve as the primary or lead coordinating agency. Follow these steps for jointly-issued, digitally-signed documents:

1. Save the finalized version of the document as an MS Word file (.docx). Be sure that the digital signatories' names and job titles are pre-inserted in the signature block area of the document.
2. Coordinate among the issuing agencies the sequence of signing; i.e., who signs first and forwards the signed file on for the next signature. Determine which agency will actually submit the signed file to OFR via the web portal once all signatures are completed.

3. The representative from the first agency digitally signs the file using the same method as a single-agency submission. See [Add Invisible Digital Signatures in MS Word](#) above. All signers must ensure that their names and job titles are pre-inserted in the signature block area of the document.
4. Email that **signed** file to the next agency for digital signature.
5. The representative from the next agency in sequence ensures that their name and job title are pre-inserted in the signature block area of the document and then digitally signs the *already-signed* file. No changes can be made to the signed file without removing the existing signature(s). If changes are required to the MS Word document, the whole process starts anew with the corrected, unsigned Word document.
6. If there are more issuing agencies, repeat Steps 4 and 5 until all agencies have digitally signed.
7. Once all agency signatures have been applied to the file, the file is sent to the agency that will submit it to OFR via the web portal. From OFR's perspective, it doesn't matter who submits the file; we're concerned with validating the digital signatories.
8. The sending agency should include a special handling letter alerting OFR of the multi-agency submission with several signatories. Be sure the special handling letter is digitally signed as well. One signer is sufficient for the special handling letter.
9. The sending agency logs into the web portal, uploads the signed MS Word file and special handling letter, and submits.
10. The signatures are validated in the web portal. We will also check all digital signatories against their printed signature block in the document. The names must match exactly or meet the accepted standards listed in the DDH. (See Step 1.)

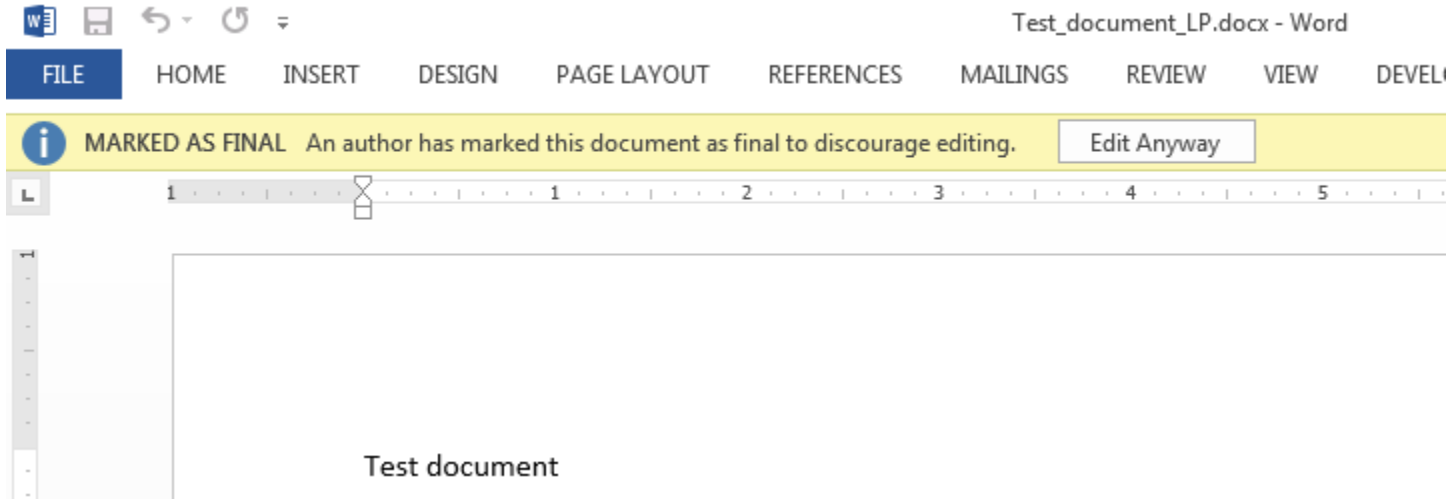
Remove Invisible Digital Signatures in MS Word

1. Open the MS Word document that contains the invisible signature you want to remove.



2. In the header, you may see the option to **View Signatures**. Click that button and proceed to Step 5. Otherwise:
3. Click the **File** tab.
4. Click **Info**.

5. Click **View Signatures**. The **Signatures** pane appears.



6. Next to the signature name, click the arrow.
7. Click **Remove Signature**.
8. Click **Yes**.

View Signature Certificate in MS Word

You can check the details of the digital certificate(s) used to sign an MS Word document (e.g., the name assigned to the certificate or expiration date).

Open the signed MS Word document containing the certificate(s) you want to check, or have the signer sign a document via the instructions provided in the [Add Invisible Digital Signatures in MS Word](#) section above.

1. In the header, you may see the option to **View Signatures**. Click that button and proceed to Step 5. Otherwise:
2. Click **Info**.
3. Click **View Signatures**. The **Signatures** pane appears.
4. In the **Signatures** pane, hover on the name of the signer you want to check; then click the small down arrow.
5. Click on **Signature Details**.
6. The signer's name as applied to the certificate is listed, along with the Certification Authority (CA). Click the **View** button.
7. A pop-up window appears. Be sure that the **General** tab is selected. The valid dates of the certificate are listed. More technical details, such as the certification path and key usage values, are shown under other tabs.

FAQs

What special software do we need to buy and install to make this work?

None. As a federal agency, you should already have MS Office 2010 or later installed. Simply follow the provided instructions to digitally sign your documents.

Do you accept any MS Word file?

No. Your file must be saved as an XML-based MS Word document (".docx"). If you're using MS Word 2010 or later, this is generally the default setting. Otherwise, when you save the file, choose "Word Document" (.docx) in the "Save as type" pull-down.



We save everything as a “.doc” file and/or we’re still using MS Word 2007 (or earlier). What are our options?

Paper-and-disk submission. Don’t forget the CD and the signed certification letter!

All we need is MS Word 2010 or later?

Yes, that and your signing credential, either the one on your PIV card or the one your agency purchased that is currently installed on your computer.

When checking for the correct certificate, as detailed in Step 7 of the [Add Invisible Digital Signatures in MS Word](#) instructions above, note the different icons for the PIV and purchased certificates:

	PIV Card certificate
	Purchased certificate

Some of our signers use MS Word for Apple on iPad. Will this work for PKI submission?

Microsoft has not put that function (PKI-based digital signature) into the MS Word for Mac (Office for Mac) software. We recognize that some agencies have signers who use the Mac platform. We expect to run testing when this function becomes available.

I already have a web portal submission account. Do I need to update it or reapply?

No.



Feedback? Create an issue on the [code repository](#) or email us at icam@gsa.gov.

Have an idea? Read our [contribution guidelines](#).

As a work of the United States government, this project is in the public domain. Copyright is also waived internationally via a CC0 1.0 waiver.

[Read More.](#)

[Privacy Policy](#)