



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

OCIO Directive 2020-003

To: Assistant Secretaries
Heads of Bureaus and Offices

From: Bruce M. Downs
Chief Information Officer (Acting)

Subject: Digital Signature Policy

Purpose

This directive establishes a Department of the Interior (DOI, Department) standard and guidelines for signing electronic documents with digital signatures. A digital signature provides a high level of assurance that the claimed signatory signed the electronic document. Documents that traditionally required notarization or wet signatures require this level of assurance.

Applicability

Currently, agencies should use digital signatures for documents that require high levels of assurance, or for convenience in lower-risk electronic documentation. This policy focuses on the use of digital signatures to provide higher levels of assurance and trustworthy records.

Background

The 21st Century Integrated Digital Experience Act (IDEA) (Public Law 115-336) and Office of Management and Budget (OMB) Memorandum M-19-21, Transition to Electronic Records, direct federal agencies to ensure that they create, retain, and manage all records in electronic format.

The National Institute of Standards (NIST) issues Federal Information Processing Standards (FIPS) as part of the Federal Information Security Management Act (FISMA) of 2002, and these standards are compulsory for federal agencies. Digital signature implementations must comply with the FIPS 186-4, Digital Signature Standard.

Policy

The Department's Digital Signature Standard is comprised of using DOI Access Cards (PIV Cards) to apply digital signatures as the authorized digital signature method. The following bullets describe how DOI will apply this standard:

- 1. Using Digital Signatures within DOI.** DOI requires personnel to use authorized digital signature methods to electronically sign documents involving transactions that require high levels of assurance (such as agreements and forms involving funds, contracts, or other documents that commit the Department to some form of legal liability).
- 2. Using Digital Signatures with External Organizations.** DOI personnel may use authorized digital signature methods to electronically sign documents and forms with non-federal government organizations contingent on the recipient's approval of this

format. DOI personnel may not require non-federal government organizations or individuals to accept or use digital signatures, therefore, they must accommodate the use of wet-ink or notarized signatures as appropriate when an external recipient rejects the digital signature.

- 3. Exceptions:** This policy does not require the use of digital signatures for low assurance transactions, documents, and forms; therefore, current practices (e.g., using government email messages) remain acceptable. Alternative digital signature methods may be acceptable upon approval by the Office of the Chief Information Officer and the Office of the Solicitor, see Frequently Asked Questions (FAQs) in Attachment 1.

Effective Date

This policy is effective immediately upon the date of signature and supersedes all previous digital signature policies, guidance, and practices that conflict with the required level of assurance.

Authorities:

- 15 U.S.C. Chapter 96, Electronic Signatures in Global and National Commerce Act
- Public Law 105-277 Sections 1703-1710, Government Paperwork Elimination Act (GPEA) (44 USC Section 3504 note)
- Public Law 115-336 21st Century Integrated Digital Experience Act (IDEA)
- OMB Memorandum M-18-21 - Transition to Electronic Records
- NIST Special Publication 800-63-3 - Digital Identity Guidelines
- FIPS 186-4 - Digital Signature Standard (DSS)

Attachments

1. Frequently Asked Questions
2. How to Add a Digital Signature Field to a Portable Document Format (PDF) File

cc: Bureau and Office Deputy Directors
Assistant Secretary Chiefs of Staff
Bureau and Office Chiefs of Staff
Bureau and Office Associate Chief Information Officers

Attachment 1

Frequently Asked Questions

Q: What is an electronic signature vs a digital signature?

A: A digital signature provides authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection as per NIST 800-63-3. The owner of a private signing key creates a "digital signature" when they use that key to create a unique mark (the signature) on an electronic document or file. The recipient employs the owner's public key to validate that the associated private key generated the signature. This process also verifies that no one altered the document. An Electronic signature is an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. A digital signature is a type of electronic signature.

Q: What is non-repudiation?

A: Provides proof of delivery to the sender and proof of the sender's identity to the recipient so that neither party can later deny having processed the data. [NS4009]

- Technical non-repudiation refers to the assurance a Relying Party has that if a public key validates a digital signature, that the corresponding private signature key made the signature.
- Legal non-repudiation refers to the establishment of possession or control of the private signature key.

Q: What is digital authentication?

A: Digital authentication is an information system's process of establishing confidence in electronically presented user identities.

Q: What are the Identity Assurance Levels (IAL)?

A: Based on their risk profile and the potential harm caused by an attacker making a successful false claim of an identity, agencies may select from the following three IAL options:

IAL1: An agency does not require linking the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted.

IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically present identity proofing.

IAL3: Agencies require physical presence for identity proofing. An authorized and trained representative of the Credentialed Service provider (CSP) must verify identifying attributes.

****NOTE:** Find complete definitions of the Identity Assurance Levels in the National Institute of Standards and Technology (NIST) Special Publication 800-63-3.

Q: What is meant by "low assurance" transactions?

A: In accordance with the NIST requirements, low assurance transactions are those that are lower risk based on the nature of the transaction. For example, the use of a login name and password verifies access to a system.

Q: Can I use the DOI Access Card to sign/approve forms from other federal, state, or local agencies or from members of the public?

A: You can use the DOI Access Card to sign an electronic document if the source organization will accept the use of the electronic signature. You should verify acceptance of the electronic signature with the source organization prior to signing the document.

Q: How do I digitally sign a document?

A: Many software applications (e.g., Microsoft Word, Adobe Acrobat) support the use of digital signatures including using the DOI Access Card, but it is important to configure the documents to prevent changes to a valid, digitally signed document. See Attachment 2 for instructions on applying digital signatures to PDF documents. Access [PIV Usage Guides/Digitally Sign a Microsoft Word Document](#) for instructions on how to sign Microsoft Word documents.

Digitally signed documents must be locked at signing to ensure the content is not modified.

Q: Can I use Alternative Digital Signature Standards and Methods?

A: If current defined and accepted methods approved for use by DOI are not useable or acceptable in certain cases DOI personnel may request approval for alternative digital signature standards and methods. The requesting official must complete a risk assessment with their Bureau or Office Associate Chief Information Officer (ACIO), or their designee to determine the appropriate identity assurance level (IAL). This risk assessment will assist in determining the appropriate alternative methodology to use with external parties that do not have a DOI Access Card, (e.g. the general public). The Office of the Solicitor must approve all alternative standards.

Q: What is the process for completing a risk assessment to utilize other digital signature technologies?

A: Using Table 1 below, evaluate the category of transaction you intend to conduct based on the electronic signature. If the evaluation requires either non-repudiation of the signature, or authenticity of the document, and the signers do not have a government issued PIV card to apply a digital signature, then you can select a different technology. Contact your bureau or office ACIO to determine if your agency already has approved digital signature technologies beyond the government issued PIV card and if you can use those technologies. If the current technologies are not acceptable, then your ACIO and staff will assist you in completing the risk assessment with the OCIO and the Office of the Solicitor to meet your specific needs.

Table 1

Category	Relationship (Internal or External)	Transaction Value *	Minimum Level of Assurance and Security	Preferred Method of Assurance and Security
1	Intra-agency (within the same Federal agency)	Funds Transfer; Contracts w/Financial or Legal Liability; PII/CUI; and/or Legal Liability	Password Token (no digital signature required; but must log into and use an official government system to execute the transaction). (IAL 2)	PIV Card to authenticate to an official government system (however, no digital signature required). (IAL3)
2	Intra-agency (within the same Federal	No Funds Transfer; No Contracts w/Financial or Legal Liability; No	Self-asserted, and no security required. (IAL 1)	Self-asserted, and no security required. (IAL 1)

Category	Relationship (Internal or External)	Transaction Value *	Minimum Level of Assurance and Security	Preferred Method of Assurance and Security
	agency)	PII/CUI; and No Legal Liability		
3	Inter-agency (between Federal agencies)	Funds Transfer; Contracts w/Financial or Legal Liability; PII/CUI; and/or Legal Liability	Soft Token or Hard Token (digital signature required on the electronic document). (IAL 3)	Government issued PIV card used to apply a digital signature to the electronic document. (IAL 3)
4	Inter-agency (between Federal agencies)	No Funds Transfer; No Contracts w/Financial or Legal Liability; No PII/CUI; and No Legal Liability	Self-asserted, and no security required. (IAL 1)	Self-asserted, and no security required. (IAL 1)
5	DOI and state/local government agencies	Funds Transfer; Contracts w/Financial or Legal Liability; PII/CUI; and/or Legal Liability	Soft Token or Hard Token (digital signature required on the electronic document). (IAL 3)	No centralized technical solution identified.
6	DOI and state/local government agencies	No Funds Transfer; No Contracts w/Financial or Legal Liability; No PII/CUI; and No Legal Liability	Self-asserted, and no security required. (IAL 1)	Self-asserted, and no security required. (IAL 1)
7	DOI and private organizations (contractor, business, university, non-profit)	Funds Transfer; Contracts w/Financial or Legal Liability; PII/CUI; and/or Legal Liability	Soft Token or Hard Token (digital signature required on the electronic document). (IAL 3)	No centralized technical solution identified.
8	DOI and private organizations (contractor, business, university, non-profit)	No Funds Transfer; No Contracts w/Financial or Legal Liability; No PII/CUI; and No Legal Liability	Self-asserted, and no security required. (IAL 1)	Self-asserted, and no security required. (IAL 1)

Category	Relationship (Internal or External)	Transaction Value *	Minimum Level of Assurance and Security	Preferred Method of Assurance and Security
9	DOI and member of the general public	Funds Transfer; Contracts w/Financial or Legal Liability; PII/CUI; and/or Legal Liability	Soft Token or Hard Token (digital signature required on the electronic document). (IAL 3)	No centralized technical solution identified.
10	DOI and member of the general public	No Funds Transfer; No Contracts w/Financial or Legal Liability; No PII/CUI; and No Legal Liability	Self-asserted, and no security required. (IAL 1)	Self-asserted, and no security required. (IAL 1)

* NOTE: Transactions that involve funds, contacts, legal liability, or PII are a higher Transaction Value. Transactions not involving these items are a lower Transaction Value.

Q: If my bureau or office is already using another form of digital signature, can we continue to use it?

A: Currently Bureaus and Offices use numerous electronic approval/signature processes that require review and the development of a risk assessment. Bureaus and offices must complete the risk assessment within one year of the DOI Digital Signature Policy effective date and obtain approval from your ACIO and the Solicitor’s Office. If the risk assessment indicates that the system poses an acceptable level of risk, you may continue to use it as is. If the risk assessment shows an unacceptable level of risk, you must develop a plan of action and milestones to update the process to an approved method with an acceptable level of risk.

Q: When is this policy effective?

A: This policy is effective immediately upon the date of signature.

Attachment 2

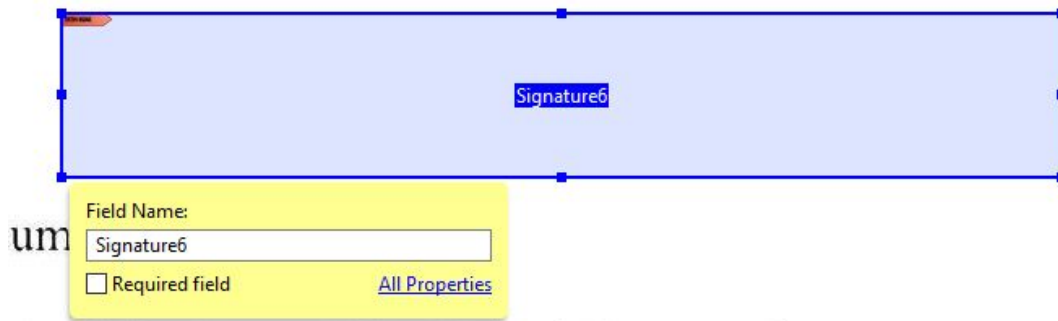
How to Add a Digital Signature Field to a Portable Document Format (PDF) File

IMPORTANT: Please ensure the PDF file that you are digitally signing is compliant with the Section 508 of the Rehabilitation Act, as amended.

1. In Adobe Acrobat *Pro DC*, open the PDF.
2. Click the Tools tab and under **Prepare Form**, click **Open**.
3. At the screen stating: “Select a file or scan a document to begin” Adobe should already display the file you opened at Step 1. If you need to change the file, then click on “Change File” and browse to the correct file.
 - **Note:** Do not check the box next to: “This document requires signatures” (it changes which signature field options are available).
 - **Recommendation:** Change the Form Field auto detection to **OFF** by clicking “Change” and unchecking the last box in **General** for: “**Automatically detect form fields,**” especially if the files you are adding the digital signature field to are not forms. If you choose to keep the “Form field auto detection is ON” you may get form fields detected in error. If this happens, click on the fields you do not need and delete them. Do not leave fields that you do not need in the file because this will affect accessibility and compliance with Section 508 of the Rehabilitation Act.
 - You may get a message: No form fields detected. This is fine, especially if the document is correspondence or the file is not a form.
4. Click **Start**.
5. On the Prepare Form ribbon over the top of the document, **click** the icon for **Add a digital signature**.



6. Your mouse will turn into a box for you to **Left mouse click > Drag a box > Release** (this is where you want the digital signature in your file).



hold the laws of the United States and to

- **Note:** If you have more than one signature in your file, you must give each digital signature field a unique name. **Check** the box next to: “Required field” if applicable, and **type** “[Person’s Name] Signature” in the Field Name. **Click** on the “All Properties” hyperlink. **Enter** “[Person’s Name] Signature” in both the Name and Tooltip fields on the General Tab. **Hit the enter key.**
7. Click **Preview** to see what the digital signature field looks like for your recipient. If you want to edit the field, click **Edit** and you will return to the editing screen. If you are satisfied with the location and size of the box, then from the Preview or Edit screen, you may save the file.
 - **Recommendation:** Do not overwrite your original file. Change the filename and save a separate file.
 8. Congratulations, you prepared your PDF file for digital signature!

How to Digitally Sign a Portable Document Format (PDF)

IMPORTANT: Please ensure the PDF file that you are digitally signing is compliant with the Section 508 of the Rehabilitation Act, as amended.

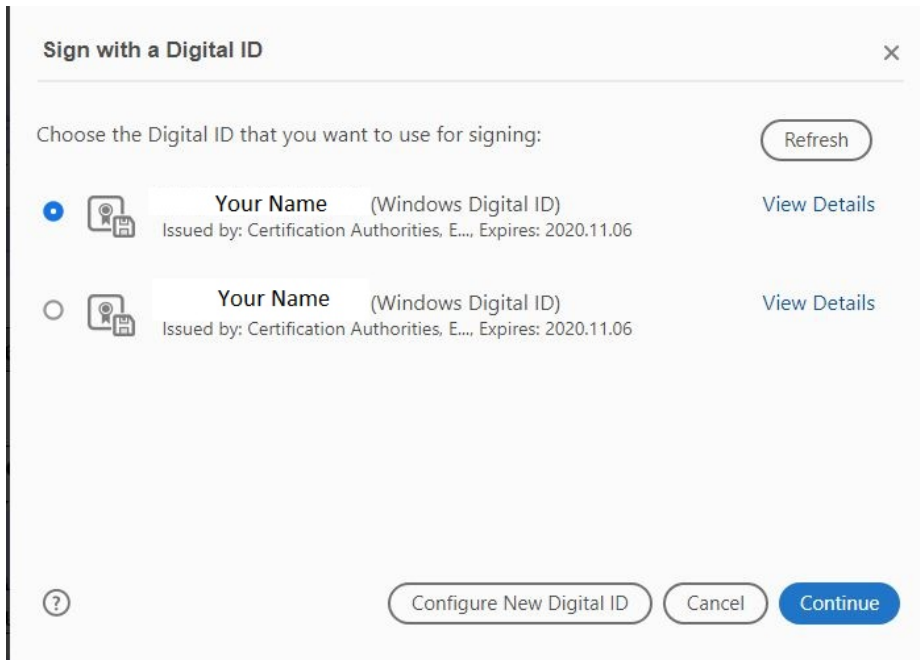
Option 1 (Preferred): To sign a PDF document that has a signature field, perform the following:

1. In Adobe Acrobat *Reader* or *Pro DC*, open the PDF you would like to sign.
2. **Click** the field that has the red sign here flag.



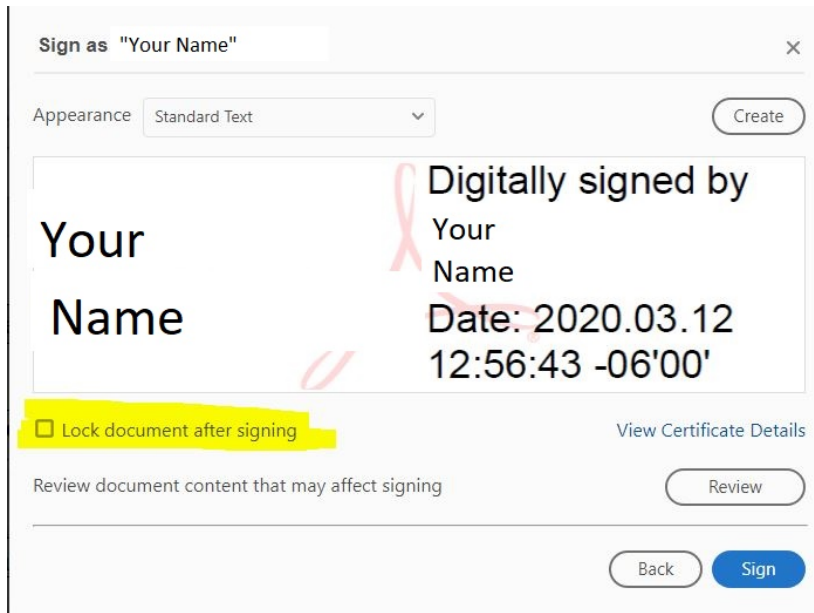
3. In the Sign with a Digital ID window, select by clicking on the digital signing certificate you would like to use, then click **Continue** (default is usually correct).

- **Note:** If there are no digital signing certificates available, then double-check that you inserted your PIV Card into your laptop or computer.



4. In the “Sign as [Name]” page of the wizard, click **Sign**.

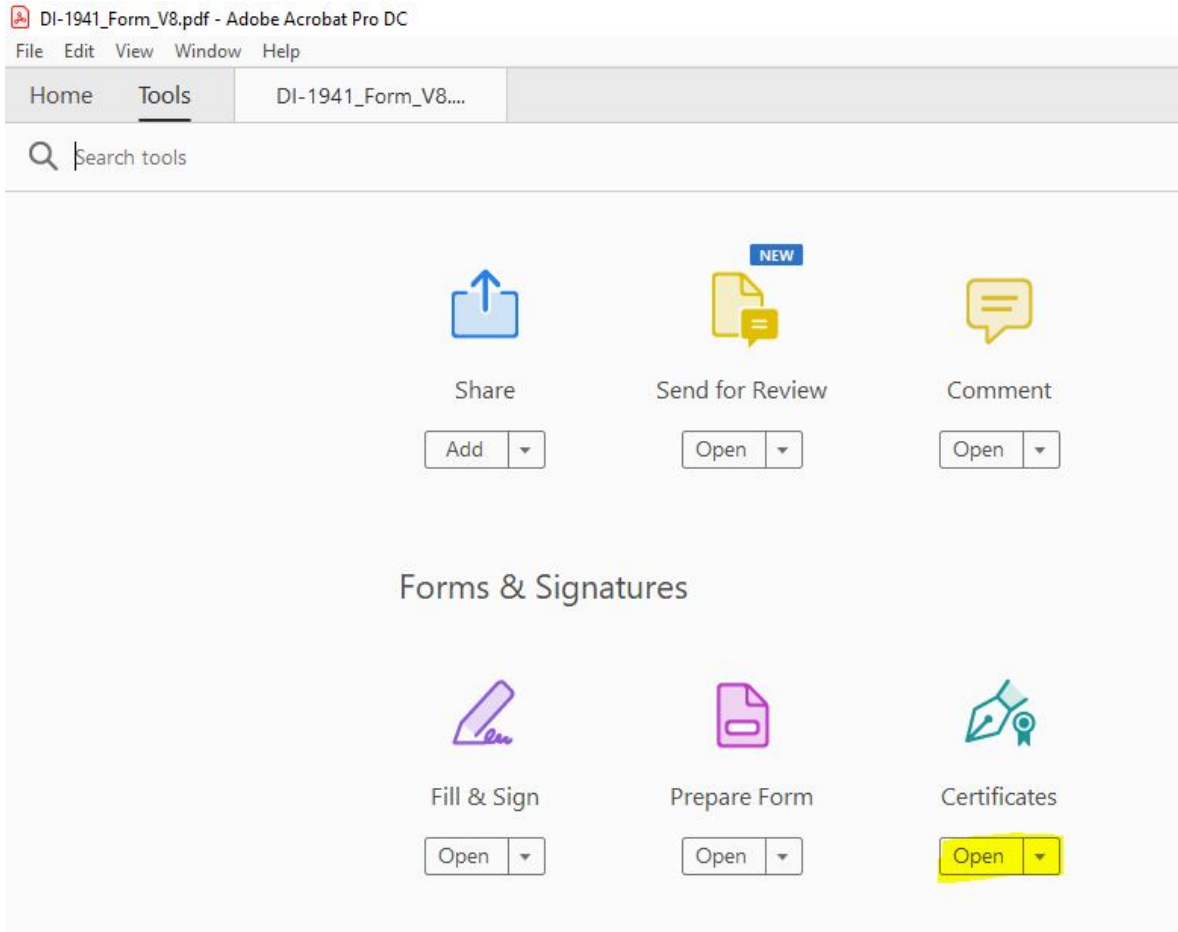
- **Note:** If you are the last person digitally signing the document, please check the “Lock document after signing” box. **This step is critical to ensure content is not modified once the document is signed.**



5. After you click **Sign** a pop-up window will appear to save your newly signed PDF file. You may overwrite the original file or add “Signed” to the filename, but you will need to save the signed file.
6. After saving the file, you may open it up you. Your digital signature will be in the location you added the box for signing.
7. Congratulations, you have just digitally signed your PDF file!

Option 2: To sign a PDF document that does not have a signature field, perform the following:

1. In Adobe Acrobat *Reader* or *Pro DC*, open the PDF you would like to sign.
2. **Click** the Tools tab and under Certificates, click **Open**.



3. On the **Certificates** ribbon over the top of the document, **click** the icon for **Digitally Sign**.



4. Using your mouse, click and drag to draw an area where you would like the signature to appear on the correspondence or in the form. Once you finish dragging out the desired area, Adobe will take you to the next step in the signing process.

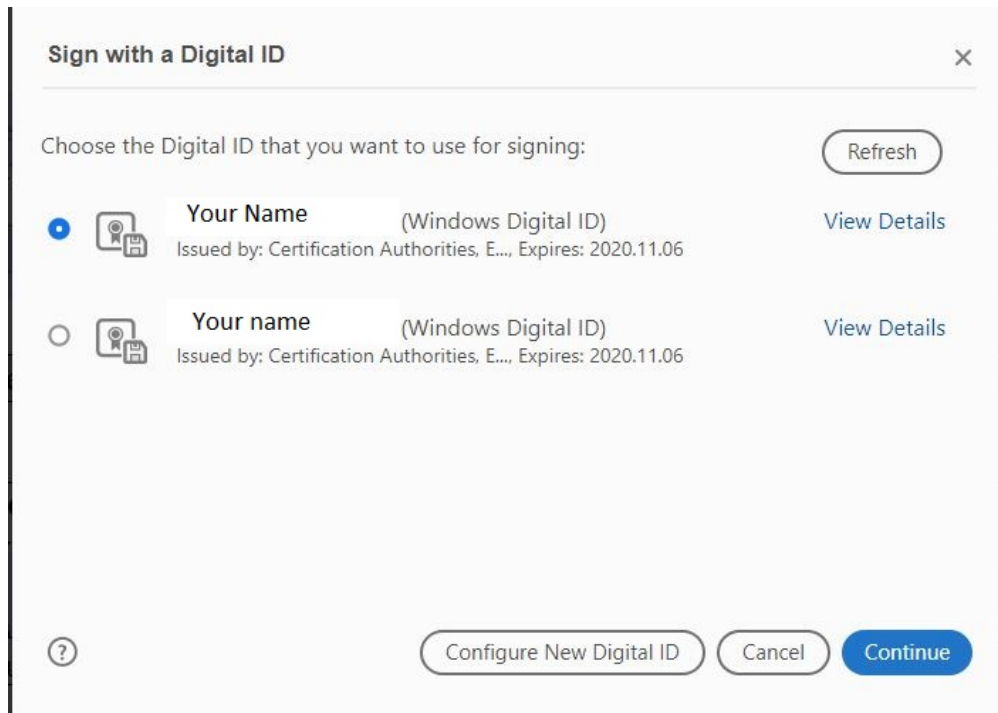
- **Note:** In the example below, I drew out a box area in the Requestor Signature box (anywhere will do). **Left mouse click > Drag a box > Release**

the scheduled retention period, required audits are completed, and there is not a
is involving these records which are known to exist.

ss	Requestor Signature
ss	Manager or Supervisor Signature

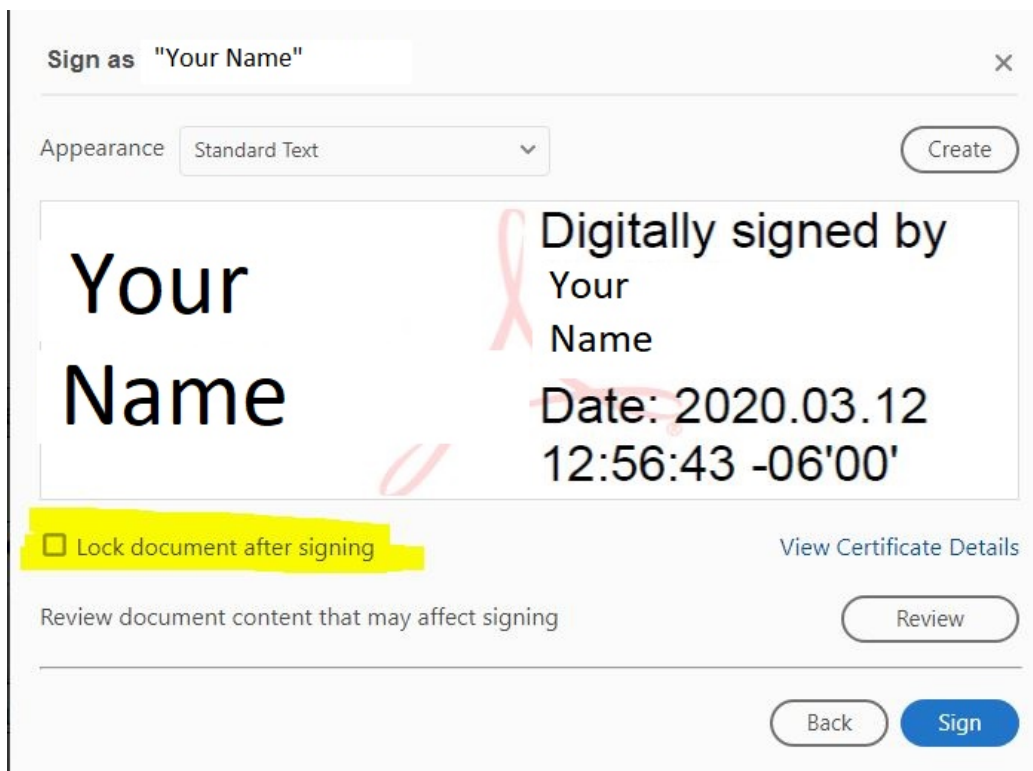
5. In the **Sign with a Digital ID** window, **click** on the digital signing certificate you would like to use, then click **Continue** (default is usually correct).

- **Note:** If there are no digital signing certificates available, then double-check that you inserted your PIV Card into your laptop or computer.



6. In the Sign as page of the wizard, click **Sign**.

- **Note:** If you are the last person digitally signing the document, please check the “Lock document after signing” box. **This step is critical to ensure content is not modified once the document is signed.**



7. After you click **Sign** you should get a pop-up window to save your newly signed PDF file. You may overwrite the original file or add “Signed” to the filename, but you will need to save the signed file.
8. After saving the file, you may open it up you. Your digital signature will be in the location you drew the box for signing.
9. Congratulations, you have just digitally signed your PDF file