

DIGITAL SIGNATURES – ePLANS REVIEW

Building a Digital Signature to
Meet State Statute Requirements
Using a Certificate Authority

Adobe Acrobat Pro DC

Adobe Reader DC

(Released July 2015)

DIGITAL SEAL AND SIGNATURE REGULATIONS

2015 Florida Statutes

[Title XXXII REGULATION OF PROFESSIONS AND OCCUPATIONS](#)

[Chapter 471ENGINEERING - SECTION 025 Seals](#)

471.025 Seals.—

(1) The board shall prescribe, by rule, one or more forms of seal to be used by licensees. Each licensee shall obtain at least one seal in the form approved by rule of the board and may, in addition, register his or her seal electronically in accordance with ss. [668.001-668.006](#). All final drawings, specifications, plans, reports, or documents prepared or issued by the licensee and being filed for public record and all final documents provided to the owner or the owner's representative shall be signed by the licensee, dated, and sealed with said seal. Such signature, date, and seal shall be evidence of the authenticity of that to which they are affixed. Drawings, specifications, plans, reports, final documents, or documents prepared or issued by a licensee may be transmitted electronically and may be signed by the licensee, dated, and sealed electronically with said seal in accordance with ss. [668.001-668.006](#).

[Chapter 668 ELECTRONIC COMMERCE – PART 1 ELECTRONIC SIGNATURES \(ss.668.001-668.006\)](#)

668.003 Definitions.—As used in this act:

- (1) "Certificate" means a computer-based record which:
 - (a) Identifies the certification authority.
 - (b) Identifies the subscriber.
 - (c) Contains the subscriber's public key.
 - (d) Is digitally signed by the certification authority.
- (2) "Certification authority" means a person who issues a certificate.
- (3) "Digital signature" means a type of electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine:
 - (a) Whether the transformation was created using the private key that corresponds to the signer's public key.
 - (b) Whether the initial message has been altered since the transformation was made.

A "key pair" is a private key and its corresponding public key in an asymmetric cryptosystem, under which the public key verifies a digital signature the private key creates. An "asymmetric cryptosystem" is an algorithm or series of algorithms which provide a secure key pair.

(4) "Electronic signature" means any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing. A writing is electronically signed if an electronic signature is logically associated with such writing

Reference: <http://www.flsenate.gov/Laws/Statutes/2015/471.025>

Reference(2): <http://www.flsenate.gov/Laws/Statutes/2015/668.003>

Florida Administrative Code 61G15-23.003 - <https://www.flrules.org/gateway/reference.asp?No=Ref-00790>

61G15-23.003 Procedures for Signing and Sealing Electronically Transmitted Plans, Specifications, Reports or Other Documents.

(1) Engineering work which must be sealed under the provisions of Section 471.025, F.S., may be signed electronically or digitally as provided herein by the professional engineer in responsible charge. As used herein, the terms "certification authority," "digital signature" and "electronic signature" shall have the meanings ascribed to them in Sections 668.003(2), (3) and (4), F.S. The affixing of a digital or electronic signature to engineering work as provided herein shall constitute the sealing of such work.

- (a) A scanned image of an original signature shall not be used in lieu of a digital or electronic signature.
- (b) The date that the electronic signature file was created or the digital signature was placed into the document must appear on the document in the same manner as date is required to be applied when a licensee uses the manual sealing procedure set out in Rule 61G15-23.002, F.A.C.

(2) A professional engineer utilizing a digital signature to seal engineering work shall have their identity authenticated by a certification authority and shall assure that the digital signature is:

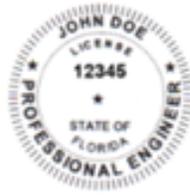
- (a) Unique to the person using it;
- (b) Capable of verification;
- (c) Under the sole control of the person using it;
- (d) Linked to a document in such a manner that the electronic signature is invalidated if any data in the document are changed

Secure Hash Standard - <https://www.flrules.org/gateway/reference.asp?No=Ref-00790>

THE DIGITAL SEAL AND SIGNATURE

An Engineer, Architect, and Surveyor's Digital Signature must be in compliance with the latest State Statute requirements **471.025 & Florida Administrative Code 61G15-23.003**. The digital signature will include a Certificate Authority and the NEW additional two sentences added by FBPE.

JOHN DOE
2016.05.16
17:04:02
'00'04-



This item has been electronically signed and sealed by John Doe PE using a Digital Signature and date. Printed copies of this document are not considered signed and sealed and the signature must be verified on any electronic copies.

A Digital Signature

The online equivalent of a notarized signature, in this case the Certificate Authority (CA) serves as the notary in terms of verifying your identity while a trusted timestamp verifies the date and time the signature was applied. Digital signatures allow users to keep their entire workflow online. Individuals can certify and sign documents as needed right from the comfort of their computers.

A Digital Signature is made up of several components:

- 1) Adobe Acrobat Standard/Pro or Reader DC** – Most Digital Signatures are built using the Adobe platform. Step one creates the digital certificate. Step two involves scanning a professional's seal into a j-peg or pdf file on the computer hard drive. When signing Adobe will integrate it with the digital certificate. Step three replaces the original digital certificate with the Certificate Authority's (CA) digital certificate file, token key or serial number in the digital ID as verification of the professional Engineer's identity.
- 2) Digital Certificate** - a way of proving your identity in online transactions and is unique to you when signing a document. The typical digital certificate includes your full name, email address and your professional qualifications for signing.
- 3) Certificate Authority (CA)** - a third party verification entity that certifies your identity with a digital certificate, software or a Token Key on a Smart Card or USB drive. Some companies require background checks or other various ways to verify your identity. The verification process can take up to two weeks.
- 4) Secure Hash** - when the Engineer clicks "sign" in Adobe Acrobat, a unique digital fingerprint (called a hash) of the document is created using a mathematical algorithm. This hash is specific to this particular document; even the slightest change would result in breaking the hash. The hash is encrypted using the Engineer's private key from the digital certificate. The encrypted hash and public key are combined into a digital signature, which is applied to the document for security.
- 5) Professional's Seal** - scan a wet stamp of the professional's seal into a 2" square j-peg or pdf file and save on the computer hard drive. **NEW! Added Language (two sentences) (1) This item has been electronically signed and sealed by [LICENSEE NAME] using a Digital Signature and date. (2) Printed copies of this document are not considered signed and sealed and the signature must be verified on any electronic copies.**

Option One – add these two sentences next to your professional seal and save as the PE Seal graphic about 2" h x 4.5" w. It will then be integrated with your digital certificate using the Adobe software. Option Two – add these two sentences anywhere on each drawing or legal document page.

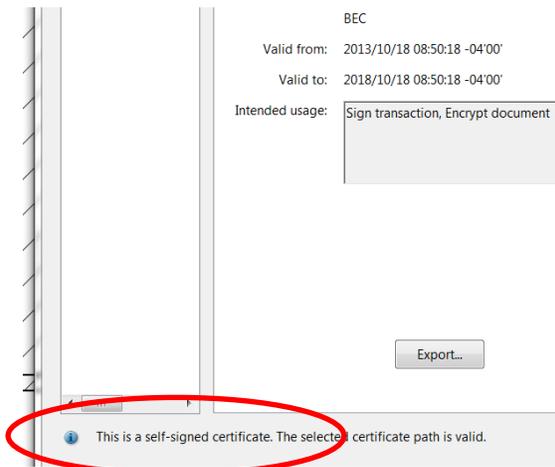
How does it Work?

When you apply a digital signature on a drawing, a cryptographic operation binds the digital certificate and the data being signed such as a PDF or other drawing file into one unique descriptor. Any change to the drawing will remove your unique descriptor or break the hash and will be indicated when opened in Adobe, stating the Signature is Invalid "This Document has been modified".

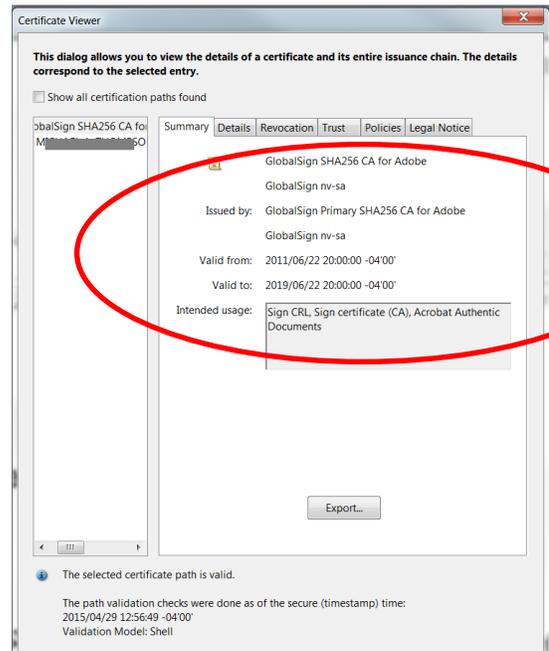
Authentication – since a third-party validated certificate is used to apply the signature, recipients can easily verify the validity of the drawing. A right click on the digital signature displays a pop up screen to validate the Public Key, Summary, Certificate Authority, Revocation, Trust, Date/Time, Signature Properties and Policies. When the drawing is opened in Adobe it will automatically try to verify the signature.

Data integrity – during the signature verification, Adobe checks to see if the data in the document has been changed since the signature was applied. Even the slightest change to the original document results a fail.

You can no longer Self-Sign your own Digital Signature. The new requirement involves having your identity, digital seal and signature validated by a 3rd party Certificate Authority. Local Engineers, Architects and Surveyors are using Adobe Entrust, IdenTrust, Cosign, DocuSign, VeriSign and GlobalSign most frequently. These companies validate your identity then have you download a new digital certificate to your computer, use software or they will send you a USB drive with a token key or serial number.



Wrong - Self Signed



Correct - Certificate Authority Attached

Create a temporary* self-signed digital ID in Adobe Acrobat Standard, Adobe Pro or Adobe Reader DC

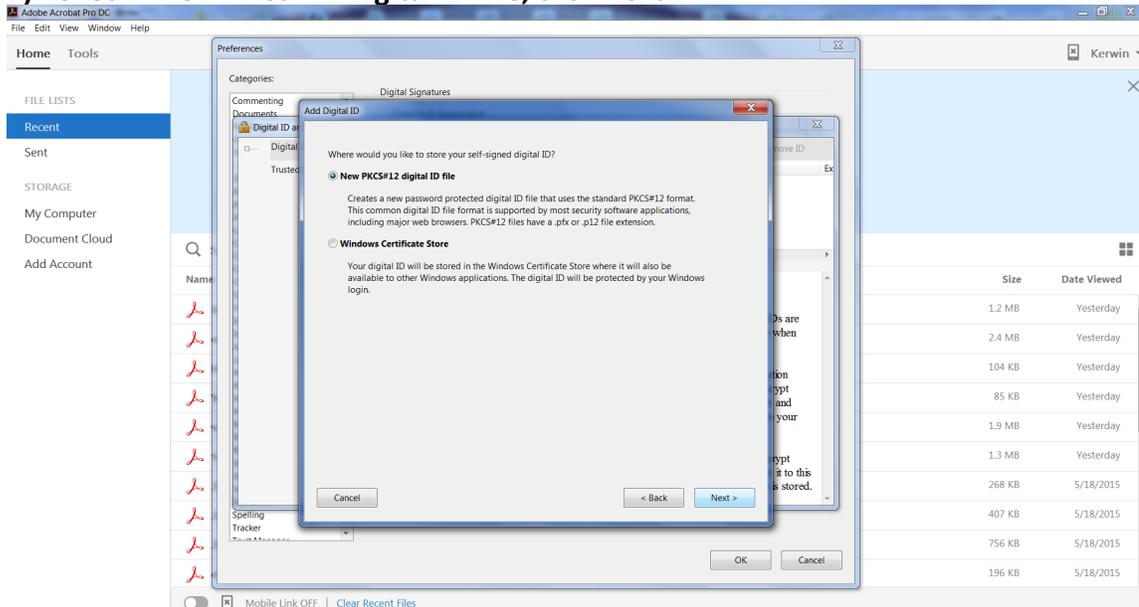
***This temporary digital ID will allow you to submit plans electronically to start the plan review process while you wait for the Certificate Authority to validate your identity. When the Certificate Authority completes their validation process they will send you a new digital certificate to replace the one you are about to build.**

How-to pdfs are also available for most versions of Adobe including Reader DC (Free) just visit our website at [ePlans Digital Signatures Guides Page](#)

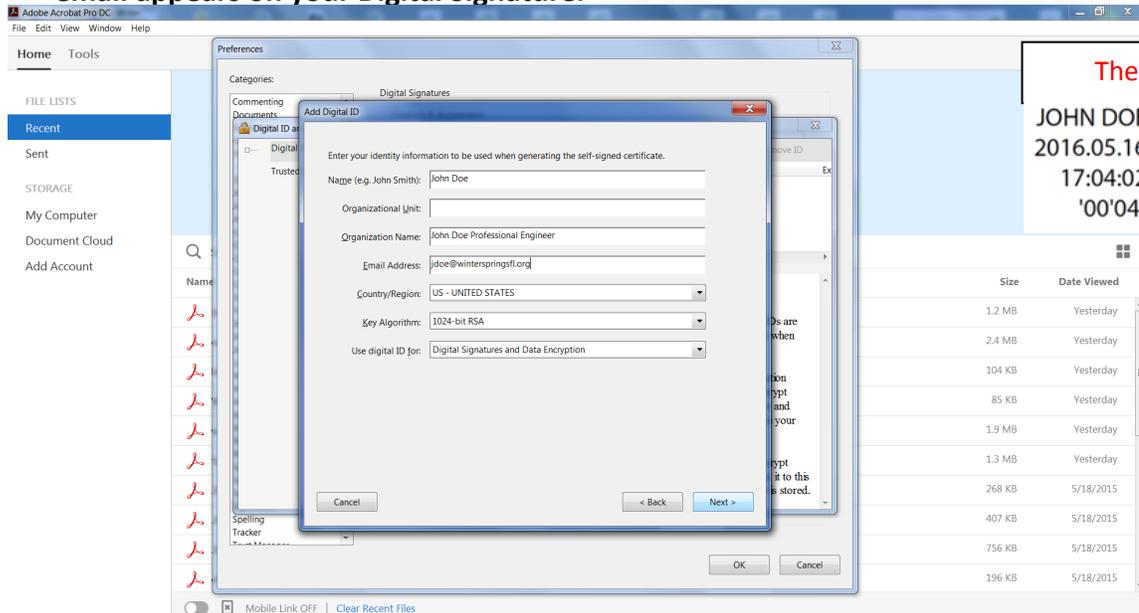
(Note: Every Adobe version may differ slightly. Some versions have you click on Security instead of Signatures in the Preferences screen below.)

Total Time needed to build a Digital Seal and Signature – about 30 to 45 minutes!

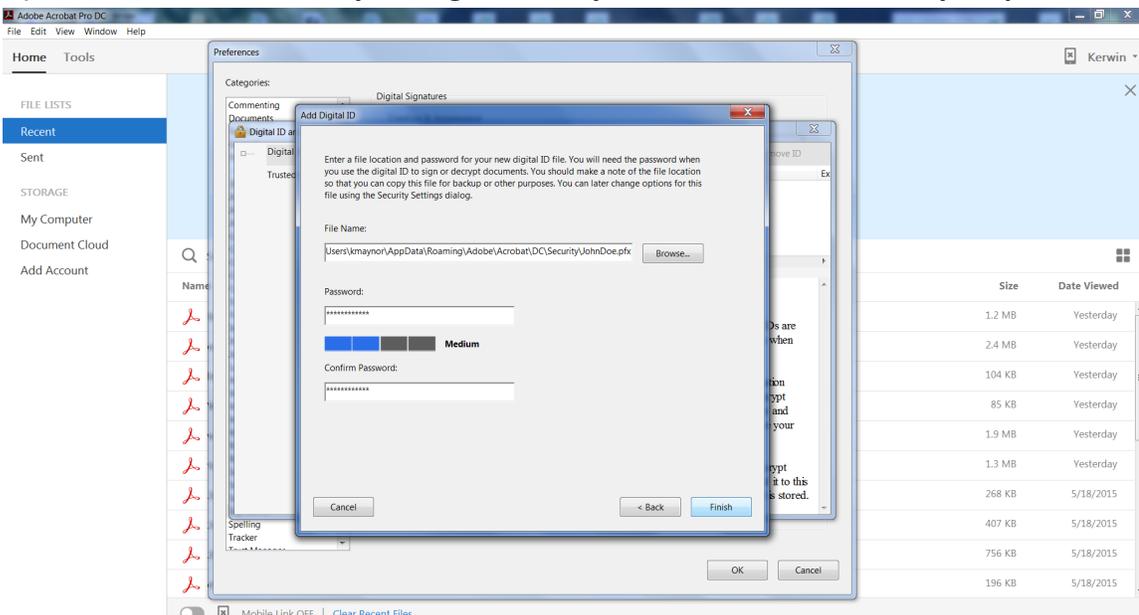
4) Check - New PKCS#12 Digital ID File, click Next.



5) Type in your identity information for your digital ID. When you certify or sign a document, the name and email appears on your Digital Signature.

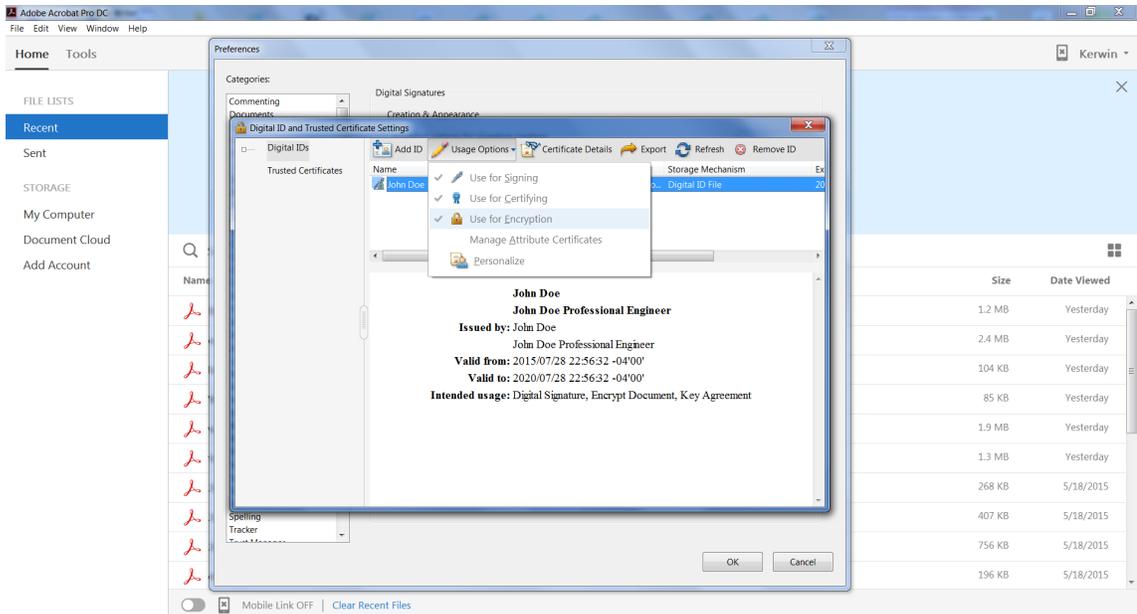


6) Choose where to save your Digital ID on your hard drive and enter your password twice, click Finish.



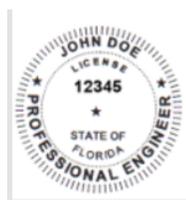
* If the “Confirm Password” entry field in step six is missing, your font sizing setting on your computer is set at +125% or higher. To expose the second password entry field you will have to cancel this ID build, go to your computer’s CONTROL PANEL > APPEARANCE and PERSONALIZATION Settings > Fonts (Make text and other items larger or smaller) setting. Adjust the setting to 100% or less, next Logout of your computer then Log back in. Repeat the Digital Signature build steps 1 thru 8 again. When the new Digital Signature is completed and tested you can re-adjust your font settings back the way they were originally set.

7) Usage Options – check Signing, Certifying, and Encryption for the Signature. (Reader will not allow all options)

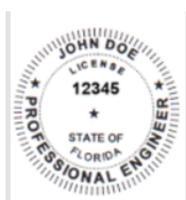


Prepare Your Seal for Import –

- a) Next, take a blank piece of 8.5 x 11 printer paper and wet seal the paper with your Professional Engineers or Architects seal. A crimp stamp can be used however, you must highlight the ruffled edges of the seal with the side of a pencil lead.
- b) Take your time and make it look nice and square as this will represent you for the next five years.
- c) Scan the seal into a graphic .jpg file and save it in an easy to find place on your computer hard drive.
- d) Crop the .jpg of your seal down to just outside the edges of the seal approximately 2”x2” square in size. We will crop it down for you if you need assistance.
- e) If you choose to add the two sentences required by FBPE to your Seal graphic you can do so now. The sentences will read: **This item has been electronically signed and sealed by [LICENSEE NAME] using a Digital Signature and date. Printed copies of this document are not considered signed and sealed and the signature must be verified on any electronic copies.**
- f) *Most Adobe versions require the graphic to be a .pdf file instead of a .jpg file.

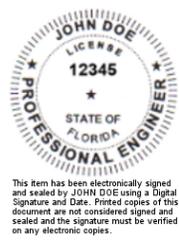


From 2”x2” to 2”x4”



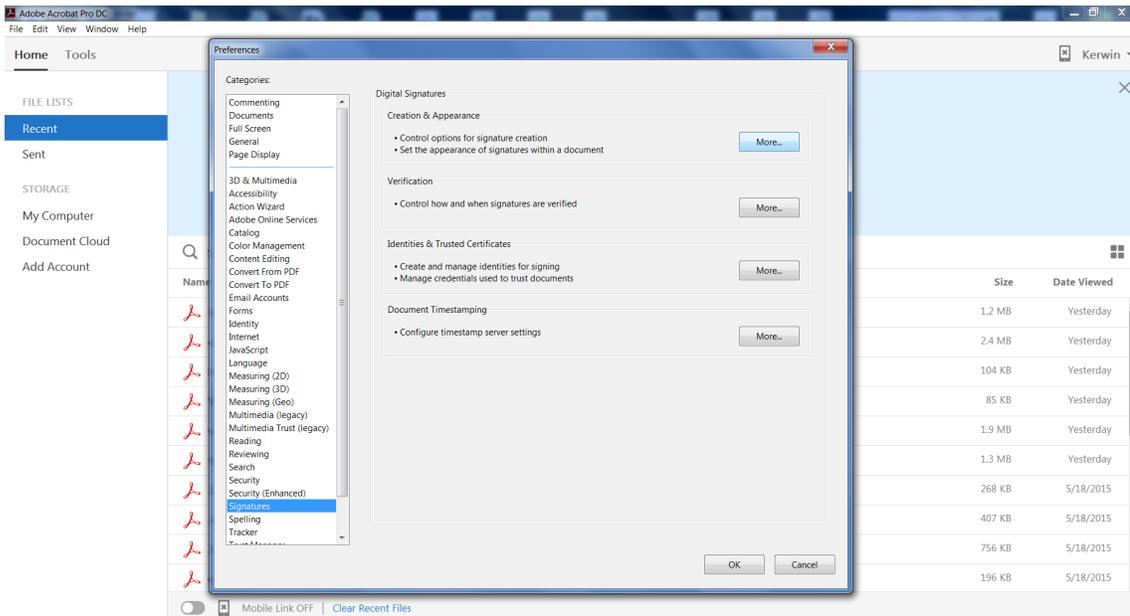
This item has been electronically signed and sealed by John Doe PE using a Digital Signature and date. Printed copies of this document are not considered signed and sealed and the signature must be verified on any electronic copies.

Or this

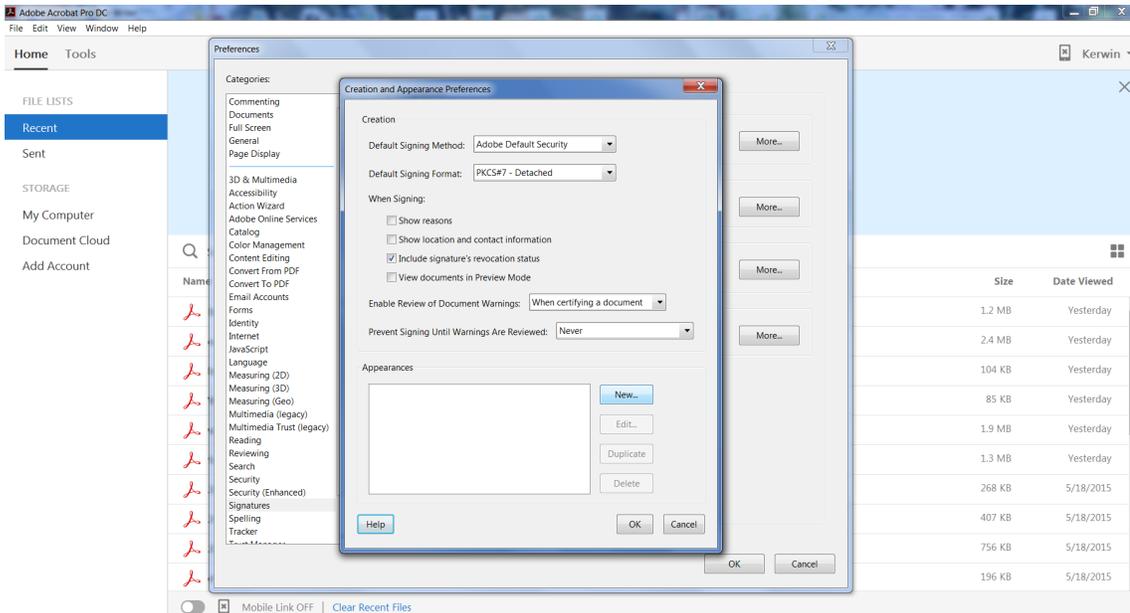


Return back to Adobe Acrobat to begin building your Digital Seal and Signature Combo appearance.

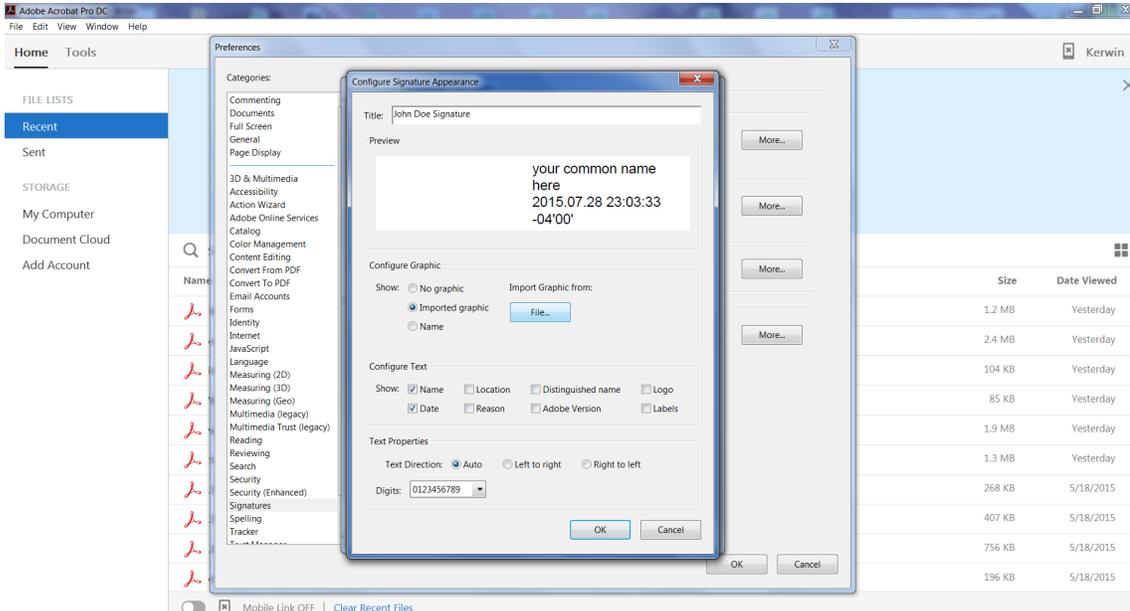
1) Main Menu>Choose Edit > Preferences > Signatures>Creation & Appearance, click More.



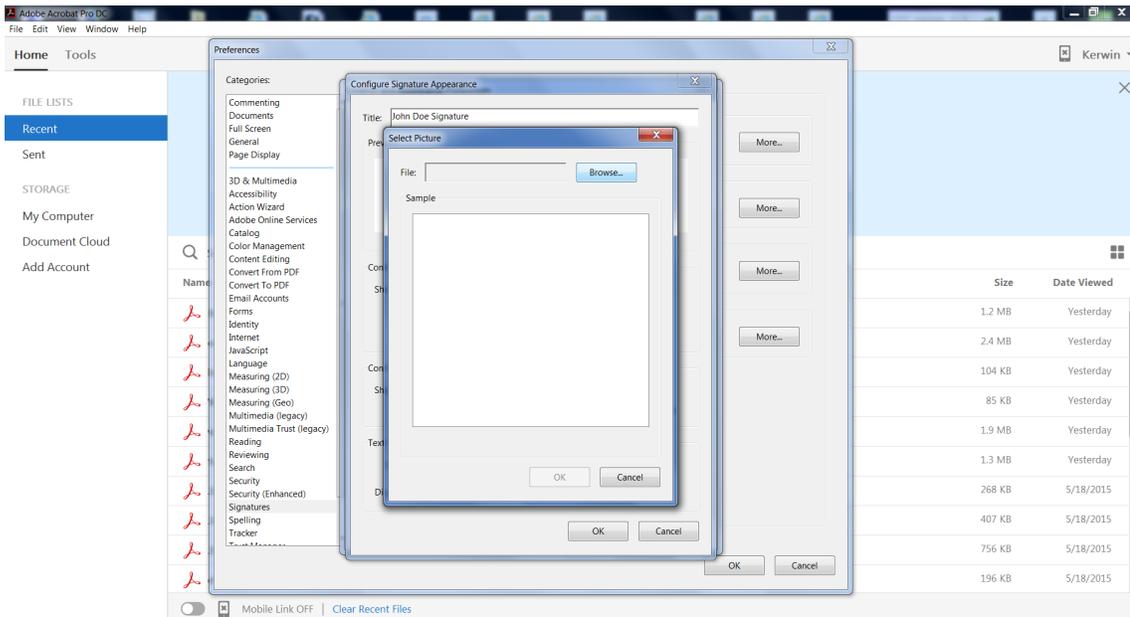
2) Choose Adobe Default Security, PKCS#7 Detached, for Appearances click NEW.



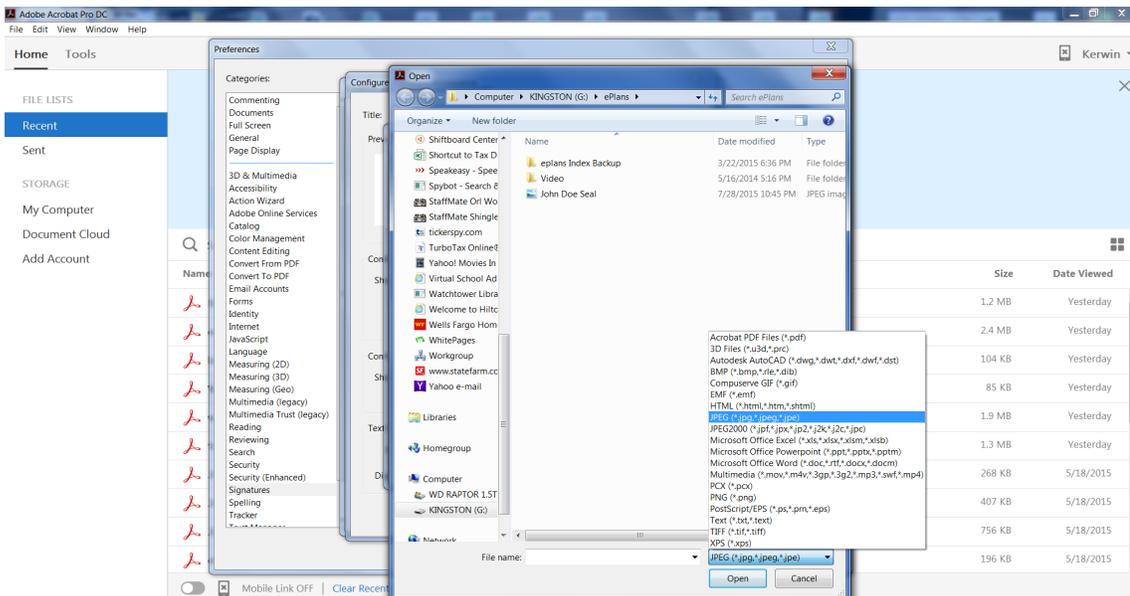
3) Type Title or description of your new Signature, choose Imported Graphic, click File.



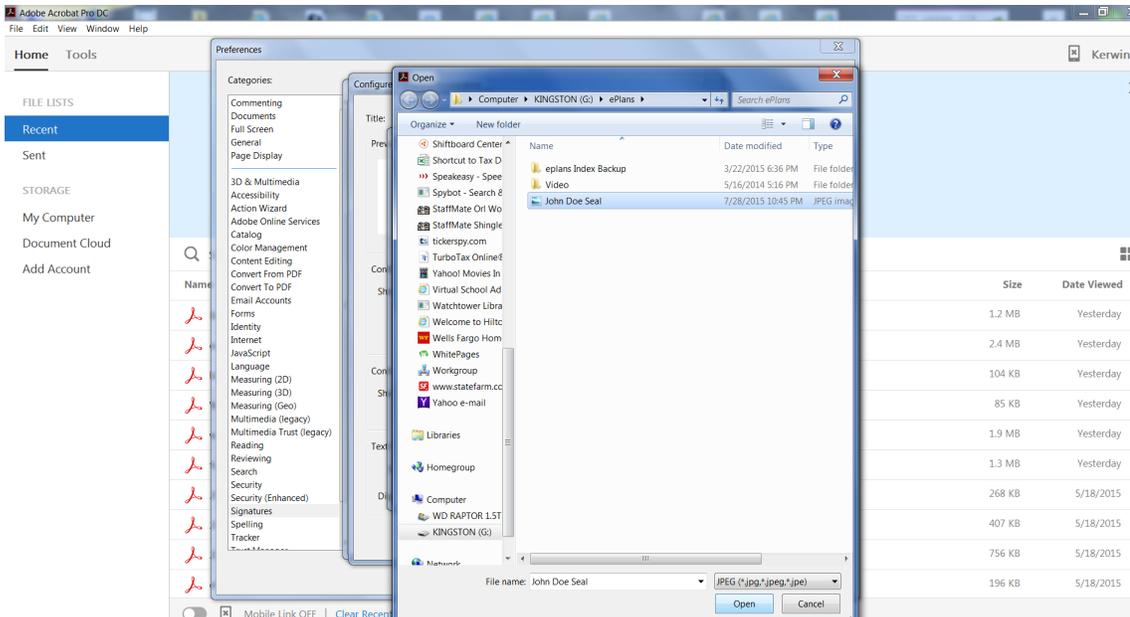
4) Click Browse to find the file location where you saved the scanned .pdf of your seal.



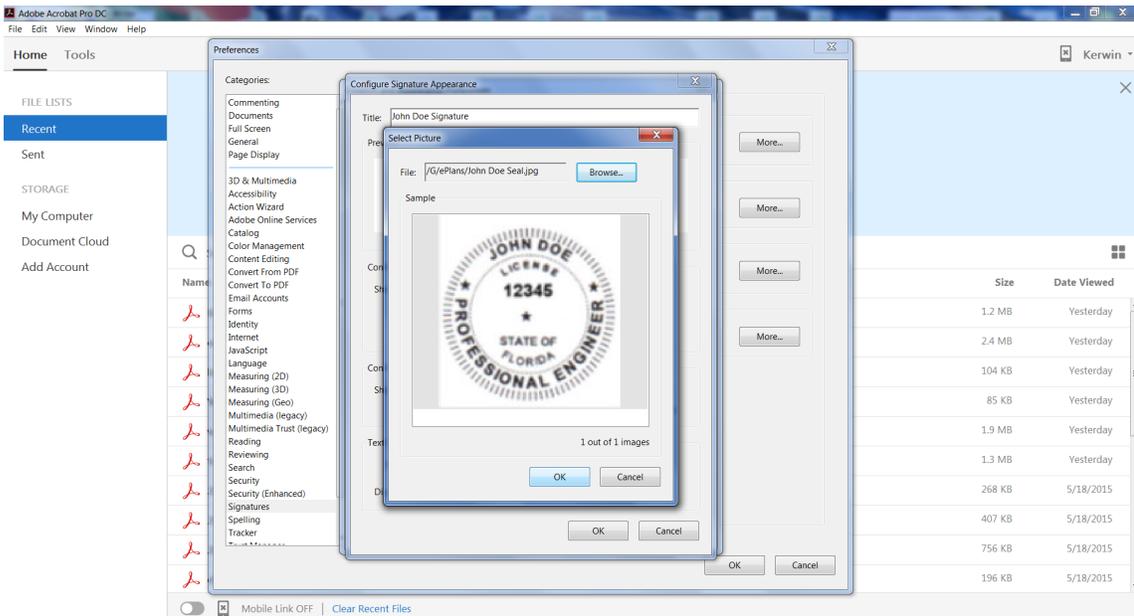
5) The File Name format can be changed from .jpg to .pdf to find your scanned seal.



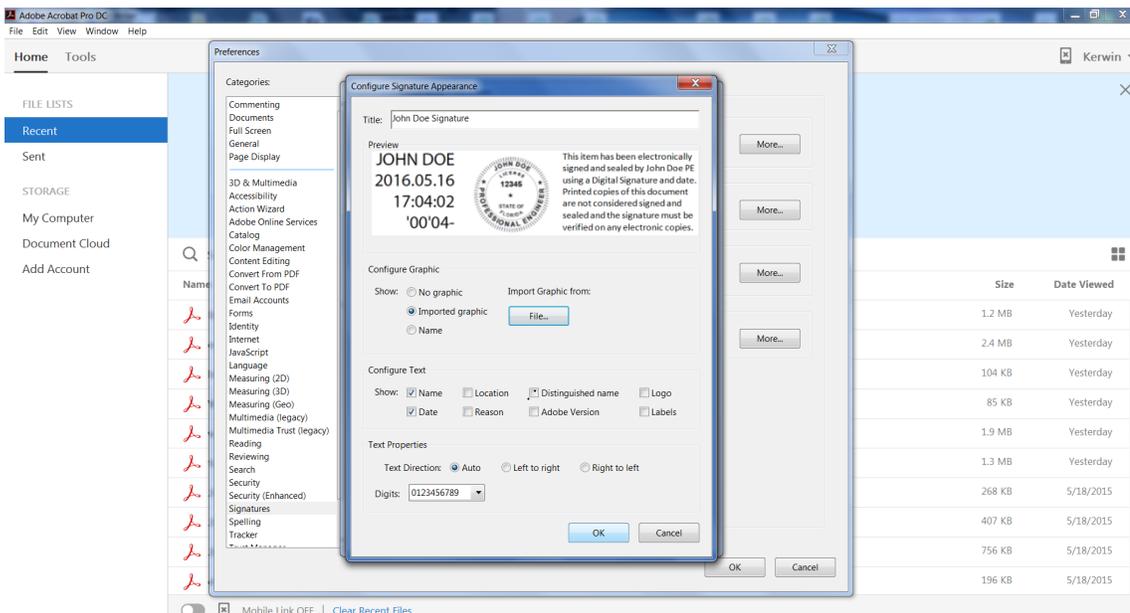
6) Select the file name of your scanned .pdf seal and click Open.



7) The Seal will appear ready for import into the digital signature, click OK.



8) Verify your seal, Check only the Name, Date, and uncheck the other six checkboxes, click OK.



Your Digital seal and signature combo is now ready to attach the Certificate Authority.

Add the Certificate Authority (CA) Verification Certificate

Certificate Authority – As mentioned at the beginning you must have a third party company verify your identity via an added digital certificate. Each company will vary in the way they verify your identity and how you receive the digital certificate. Most will have you either download the certificate or send you the certificate on a smart card or usb drive to attach to the computer you will be using to sign with.

The required digital certificate will be similar to those used by FDOT such as an Access Certificate for Electronic Services (ACES). This type will meet the Laws & Rules set by the Florida Board of Professional Engineers in Florida Statutes 471 and as implemented in Florida Administrative Code 61G15-23 for signing and sealing documents that are delivered electronically.

While we cannot recommend which third party company to use we have narrowed down the list to some of the following companies that meet the requirements for signing construction plans and are already in use by other local Professional Engineers.

For Your Information – Links to websites

Adobe - <https://acrobat.adobe.com/us/en/products/acrobat-pro.html>

Identrust – <http://identrust.com/fdot/>

Cosign – <http://www.arx.com/digital-signature/>

DocuSign - <https://www.docusign.com/products/electronic-signature>

Entrust - <https://www.entrust.com/document-signing-certificates/>

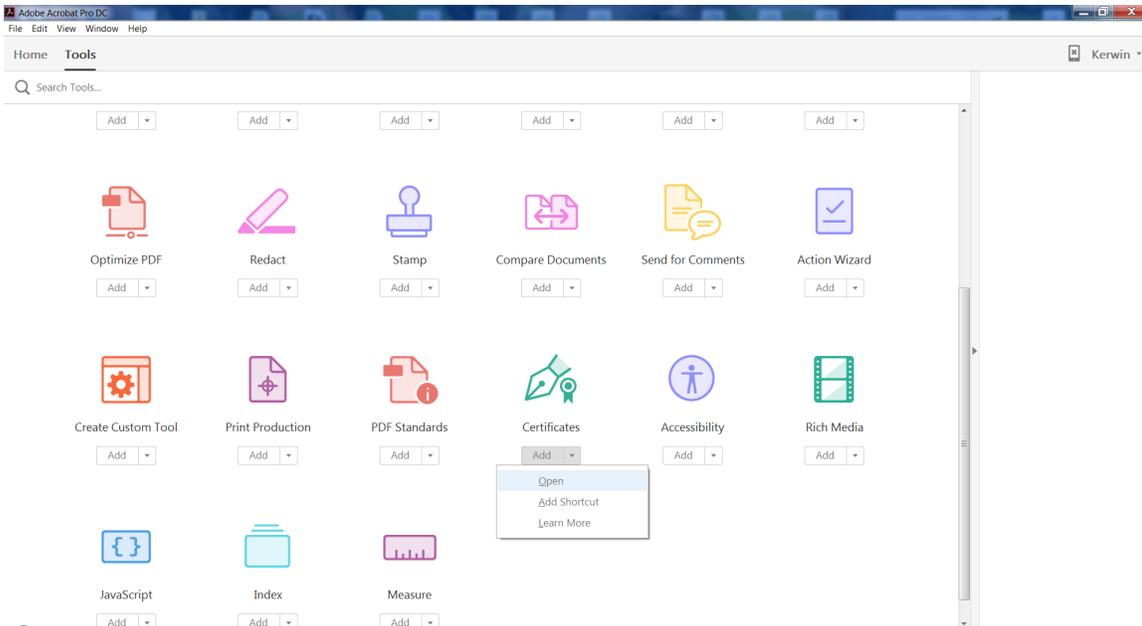
Globalsign – <https://www.globalsign.com/en/digital-signatures/>

VeriSign - <https://www.symantec.com/products/information-protection/eca-certificates/pricing>

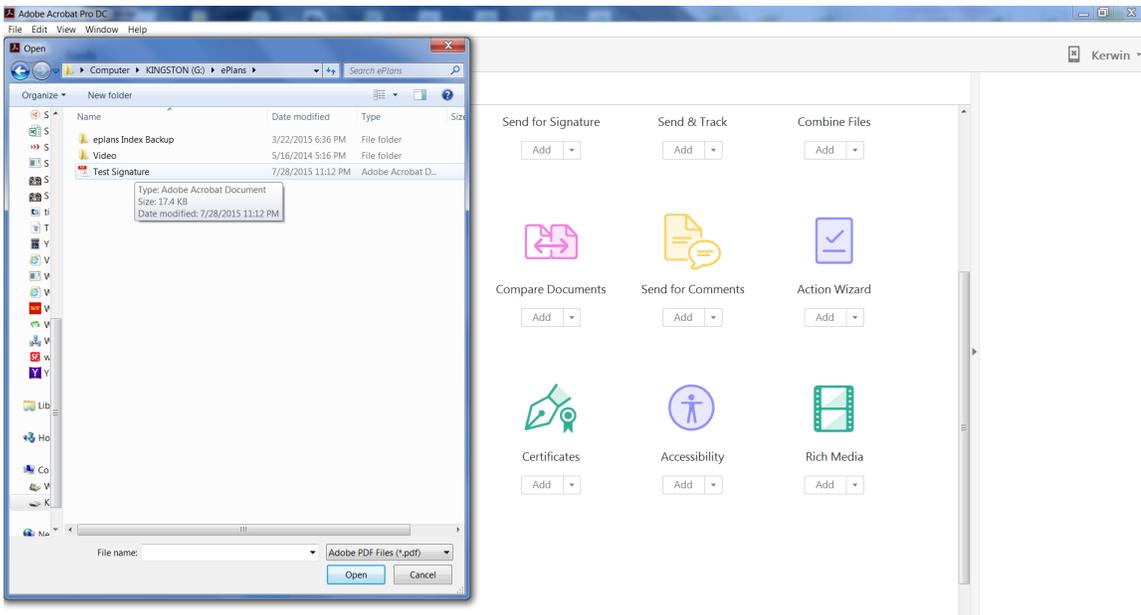
Test your new Digital Signature

You will be using Adobe Acrobat Pro DC or Reader DC to sign your drawings

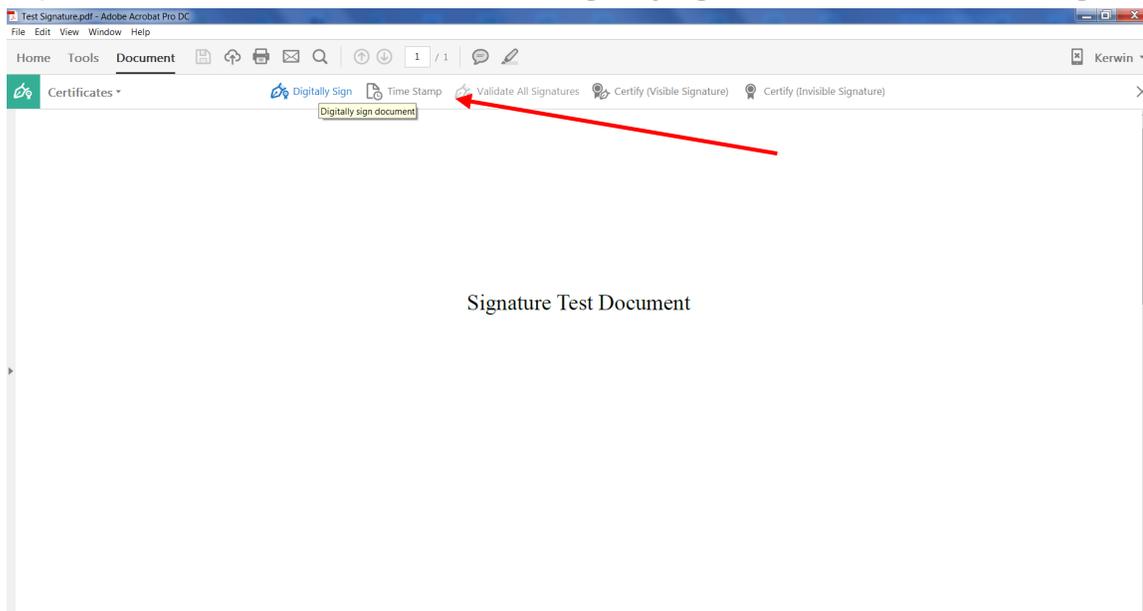
1) Select Tools on the upper left, then select the Add button under Certificates, click Open to open a document.



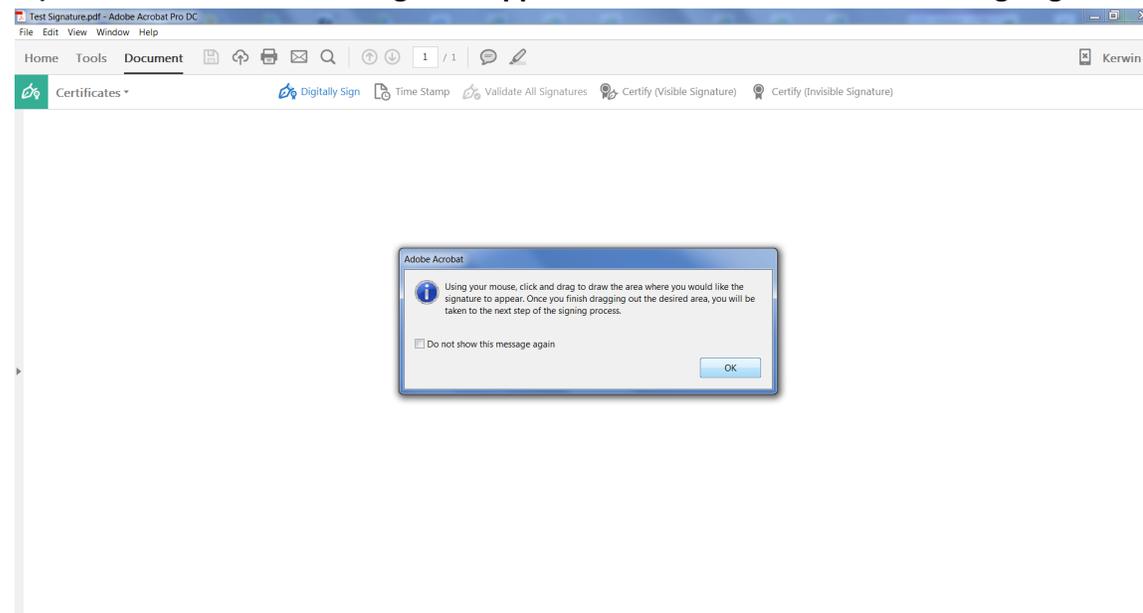
2) Select the Drawing or Document you want to test your Digital Signature on, then click Open.



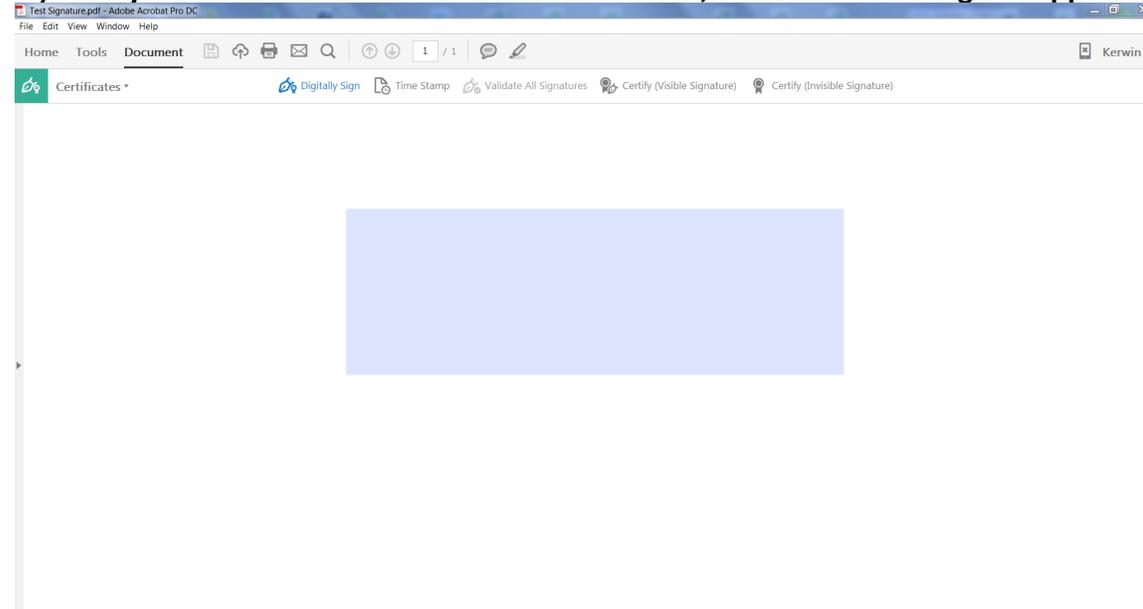
3) Your Test document will load, select Digitally Sign on the Certificates heading.



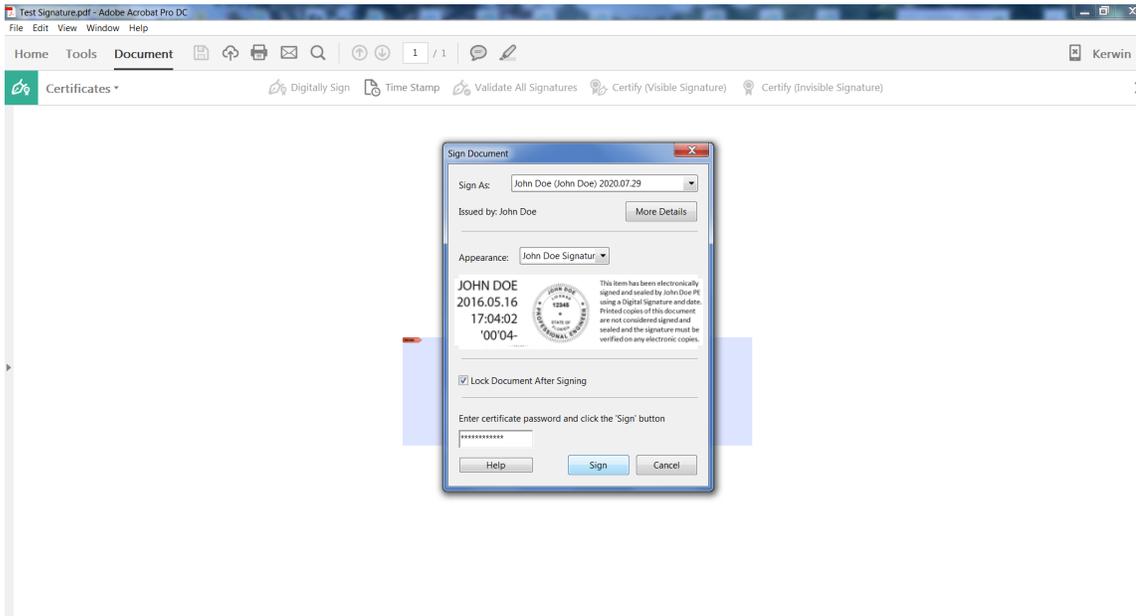
4) The draw textbox message will appear. Check Do not show this message again to save time signing, click OK.



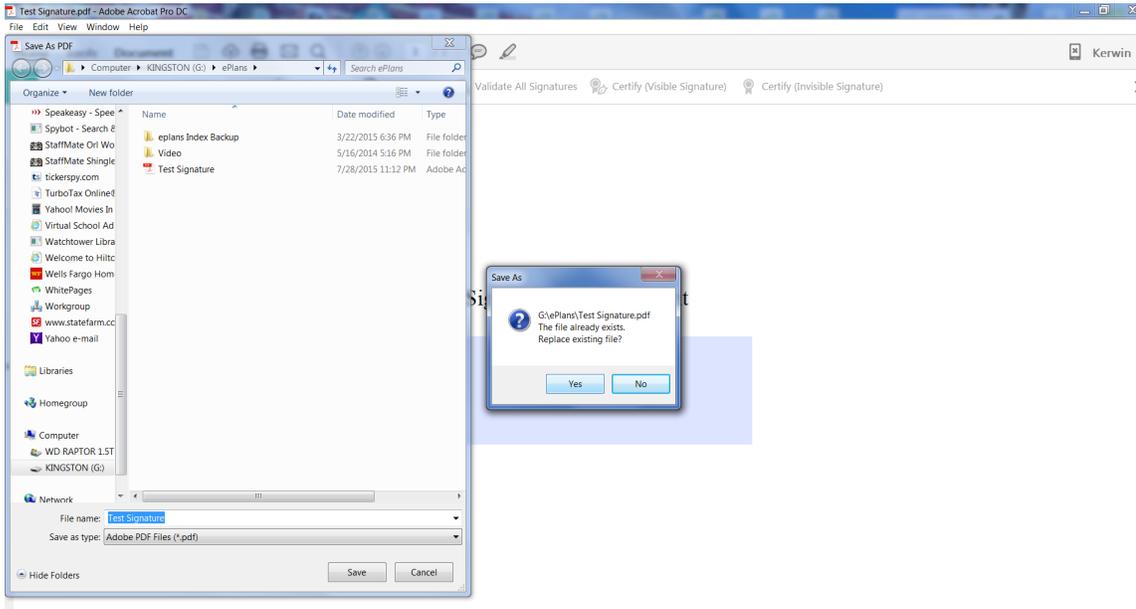
5) Use your mouse to draw a textbox about 2"x 4", if too small nothing will appear.



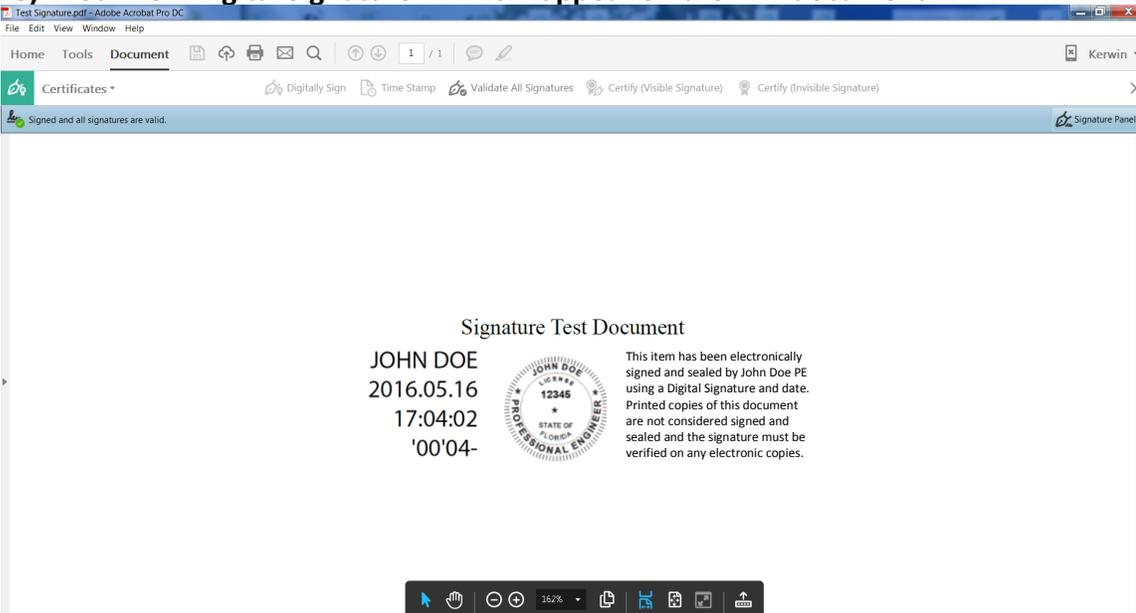
6) Select the correct "Sign As" Name and the correct "Appearance" (your New seal w/sentences), enter your password, check the "Lock" checkbox, then click Sign.



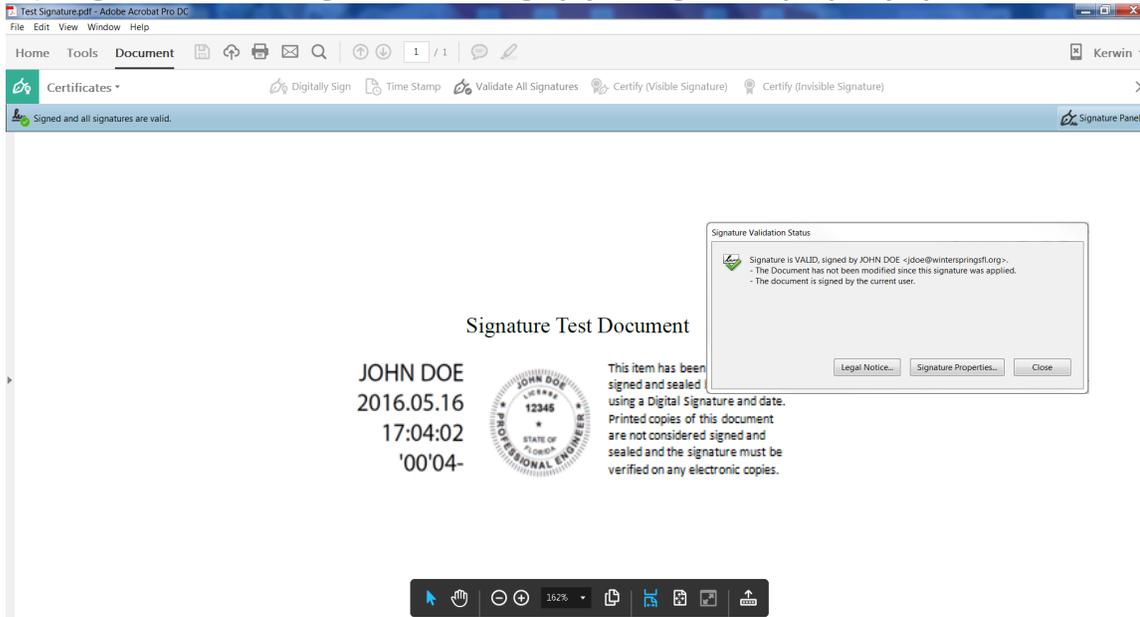
7) Select a new Save As Name to Replace the Existing PDF file. The new one will be digitally signed.



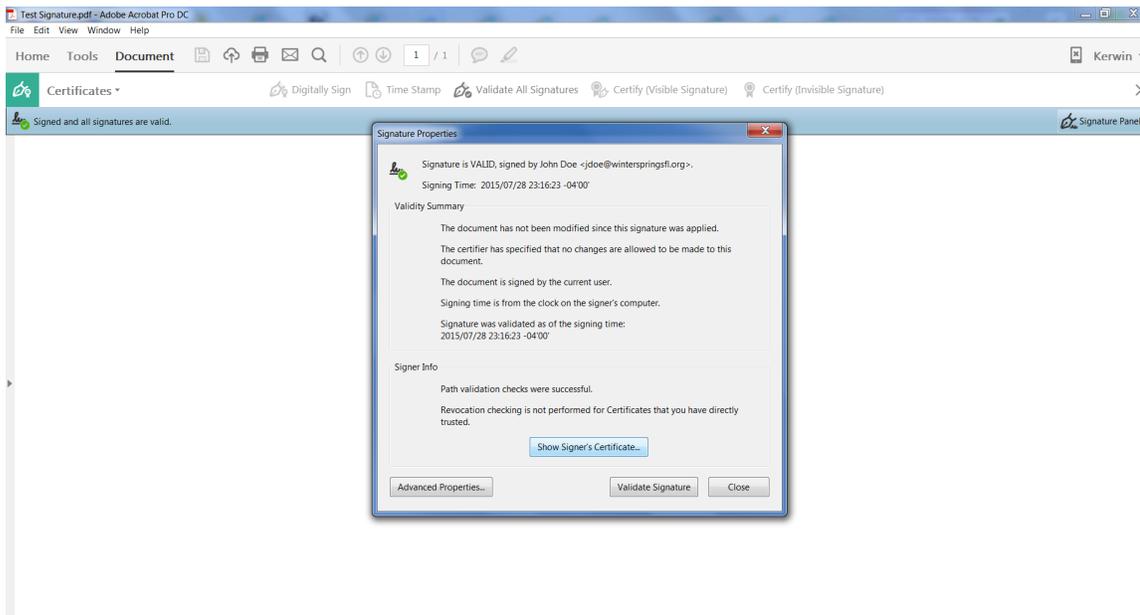
8) Your new Digital Signature will now appear on the PDF document.



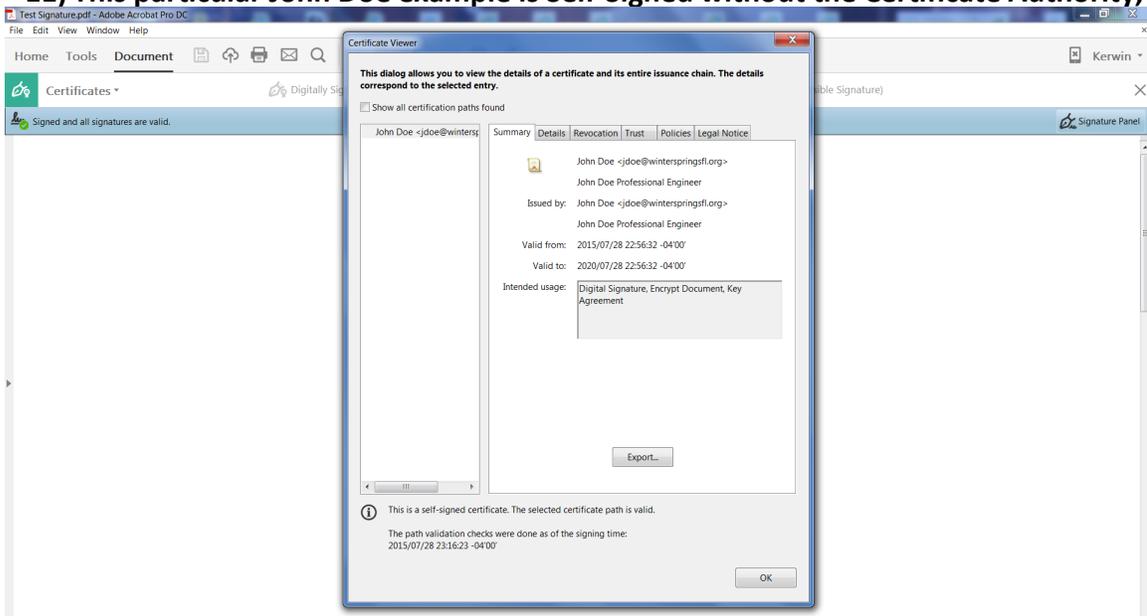
9) Right click on the signature to bring up your signature property options.



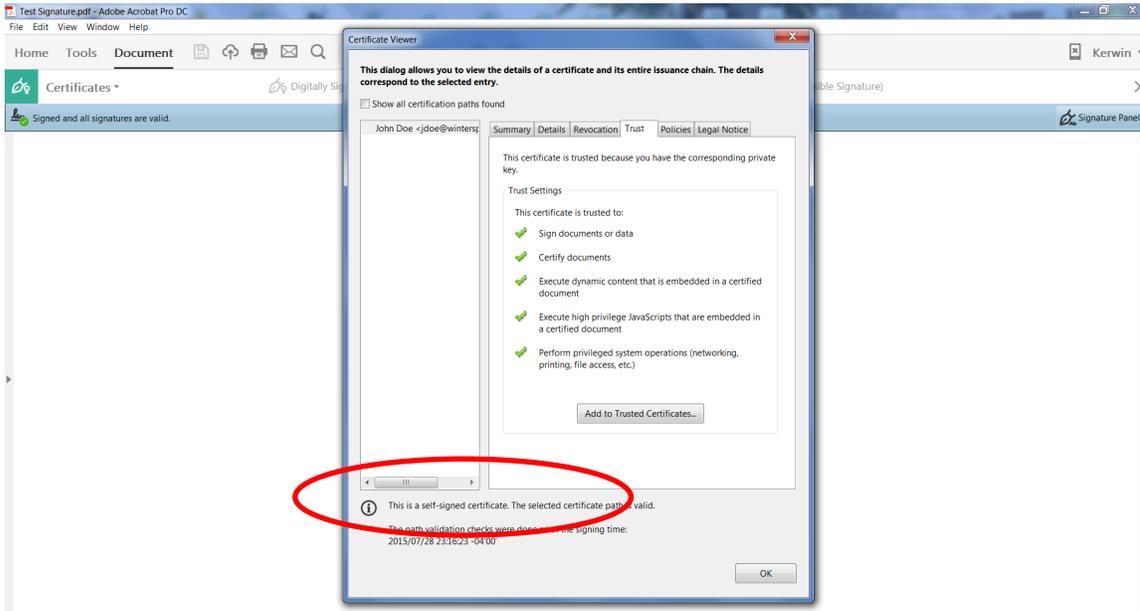
10) Click Show Signer's Certificate.



11) This particular John Doe example is Self-Signed without the Certificate Authority, the CA must be added.



12) The Trust Tab displays the Trust settings .



When the Certificate Authority attaches to your Digital Signature the self-signed certificate comment will disappear and “The selected certificate path is valid” will only appear. Also, the Certificate Authority will be listed above you name in the upper left column.

