Section 2: Digital Signatures & Seals

2.1 Digital Signatures

A digital signature is represented in a computer as a string of bits. A digital signature is computed using a set of rules and a set of parameters that allow the identity of the signatory and the integrity of the data to be verified. Digital signatures may be generated on both stored and transmitted data. A digital signature algorithm allows an entity to authenticate the integrity of signed data and the identity of the signatory. The recipient of a signed message can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory.

Digital signatures may be purchased from one of the following trusted third-party verifiers:

- Adobe Entrust
- IdenTrust
- Cosign
- DocuSign
- GlobalSign

Any design professional that wishes to use a company other than the ones listed above, may request approval from the Port Authority Quality Assurance Division. Upon satisfactorily demonstrating compliance with the criteria above, QAD will authorize submission of the digital signature from that company.

2.2 Digital Seals

Digital seals (eSeal) is an electronic image of your professional seal (i.e. jpeg, tiff, dxf). This will be integrated with your digital certificate (Digital Signature), which is applied using the Adobe Software.

Digital signatures may be purchased from one of the following companies:

- Presto Direct LLC
- Acorn Sales Company Incorporate

Example:

For more information please refer to: **THE PORT AUTHORITY DIGITAL SIGNATURE & SEAL POLICY**
****Provide PDF Link****

2.3 Digital Certificate

A set of data that uniquely identifies a key pair and an owner that is authorized to use the key pair. The certificate contains the owner's public key and possibly other information and is digitally signed by a Certification Authority (i.e., a trusted party), thereby binding the public key to the owner.

2.4 Certificate Authority

The entity in a (PKI) Public Key Infrastructure *(a frame that is established to issue, maintain and revoke public key certificates)* that is responsible for issuing certificates and exacting compliance with a PKI policy.

2.5 Secure Hash Algorithm

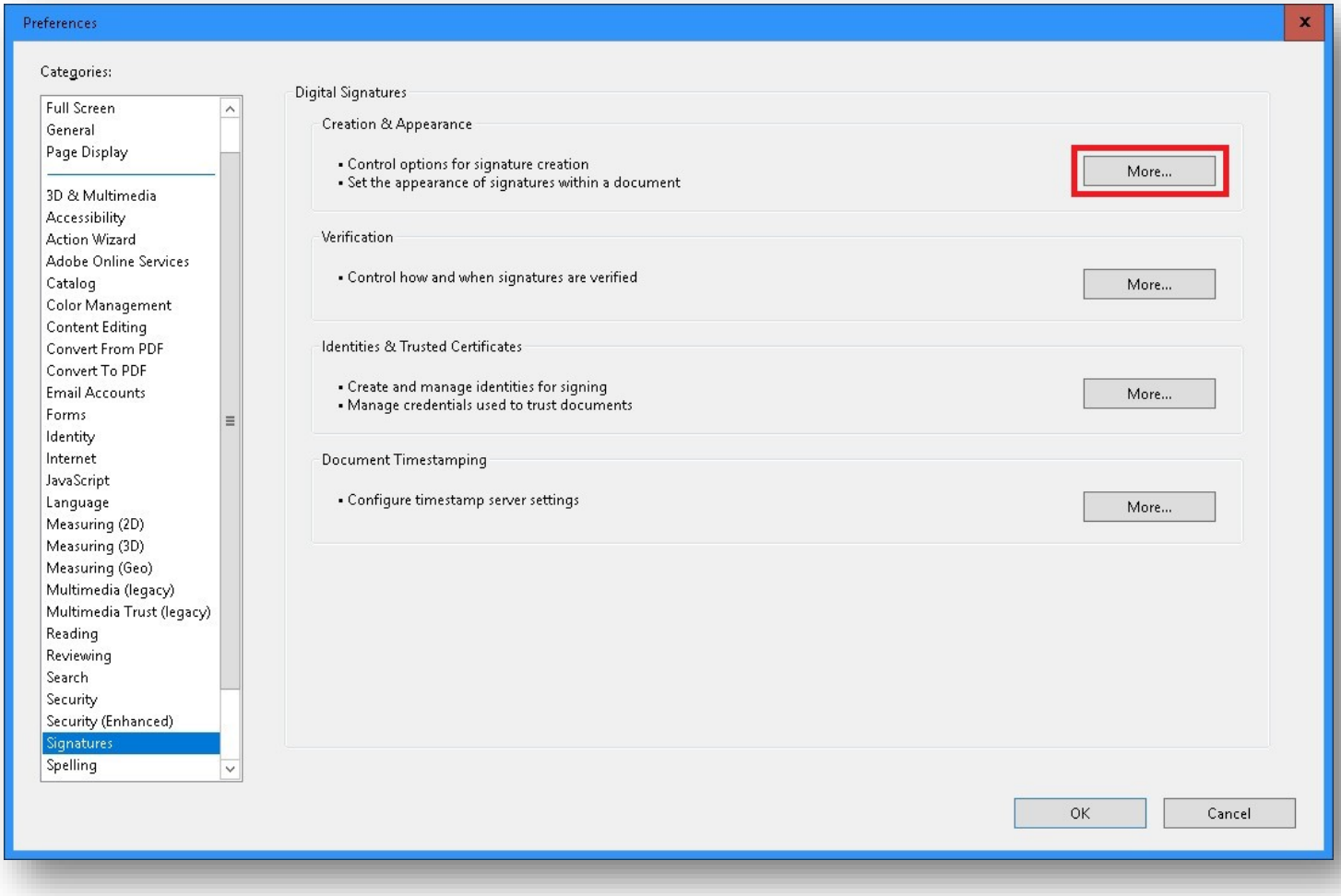
Typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits).

2.6 Setting up your Digital Seal

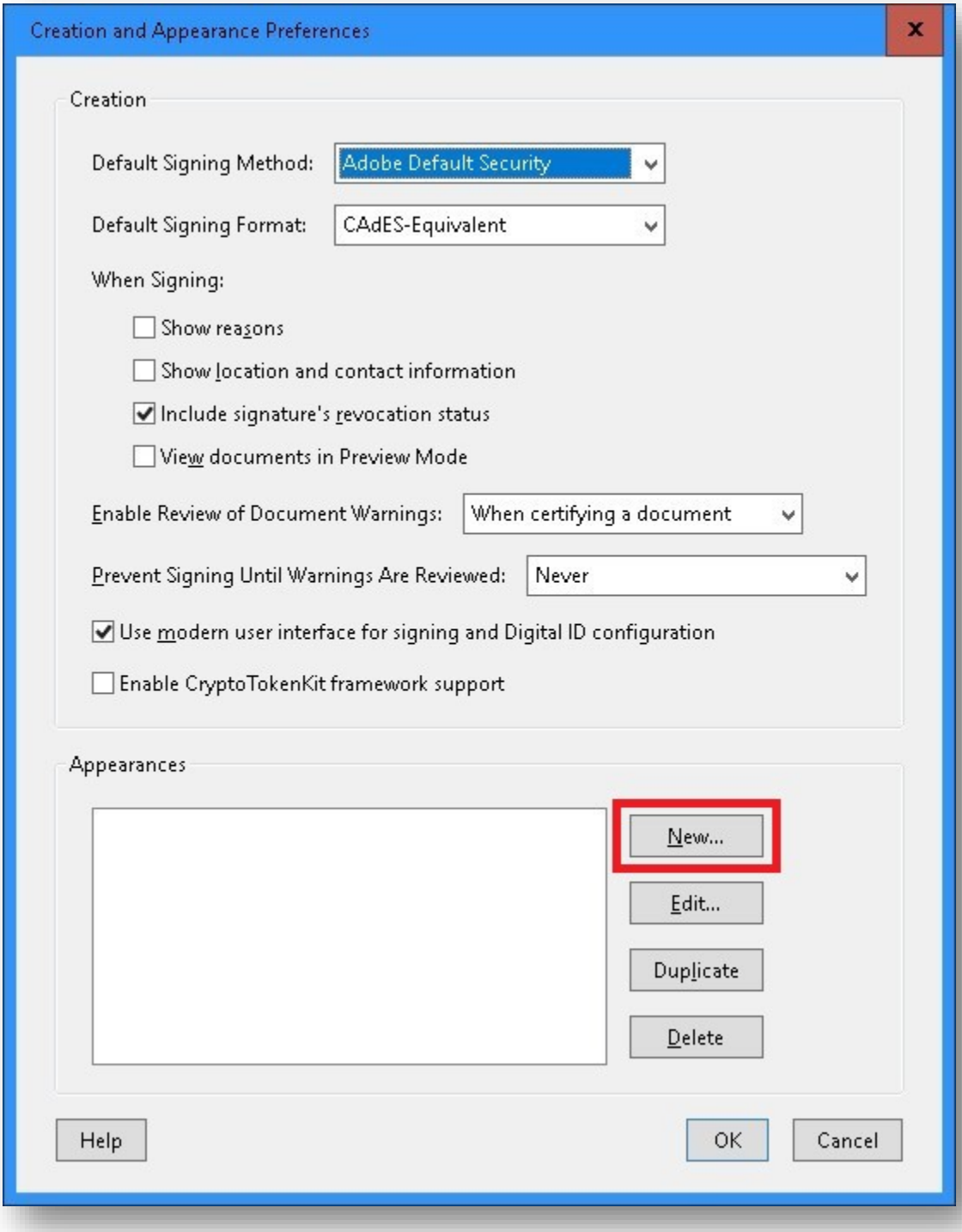
Using Adobe Acrobat Standard or Pro.
(Note: Adobe versions may differ slightly. Some versions you may need to click on 'Signatures' instead of 'Security' in the preferences below)

- From the Main Menu > Select Edit > Preferences > Signatures (or Security) > More…

- Under 'Digital Signatures' – 'Creation & Appearance' pop-up window will appear.

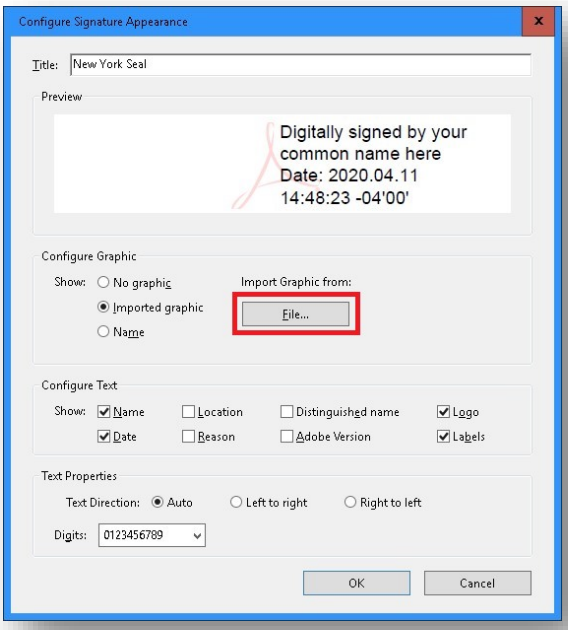


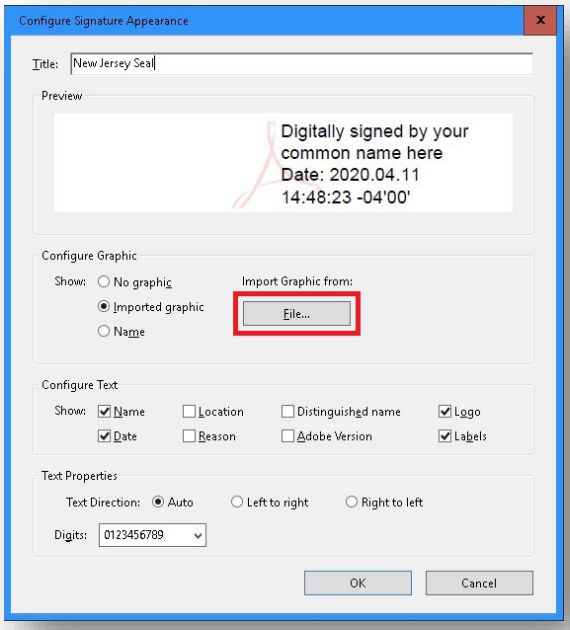
o Select 'New'


Creation and Appearance Preferences
Creation
Default Signing Method:
Adobe Default Security
Default Signing Format:
CAdES-Equivalent
When Signing:
Show reasons
Show location and contact information
Include signature's revocation status
View documents in Preview Mode
Enable Review of Document Warnings:
When certifying a document
Prevent Signing Until Warnings Are Reviewed:
Never
Use modern user interface for signing and Digital ID configuration
Enable CryptoTokenKit framework support
Appearances
New...
Edit...
Duplicate
Delete
Help
OK
Cancel

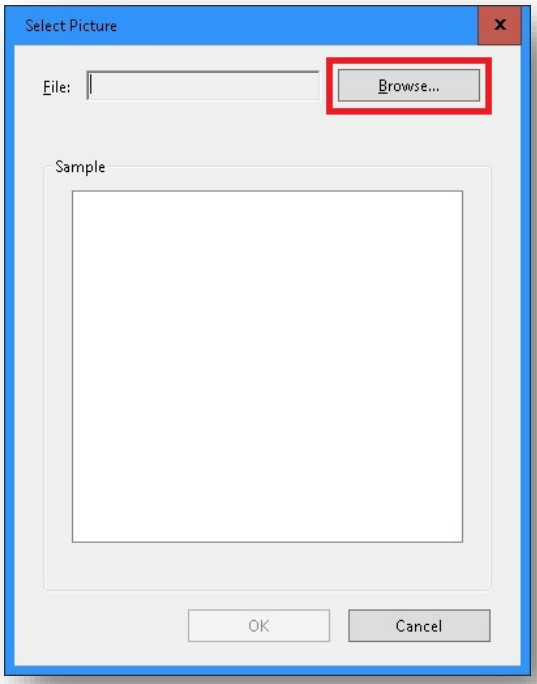
- ‘Configure Signature Appearance’ pop-up window will appear. Create an appearance for both New York Seal and the New Jersey Seal

- Configure Graphic > Import Graphic > File…

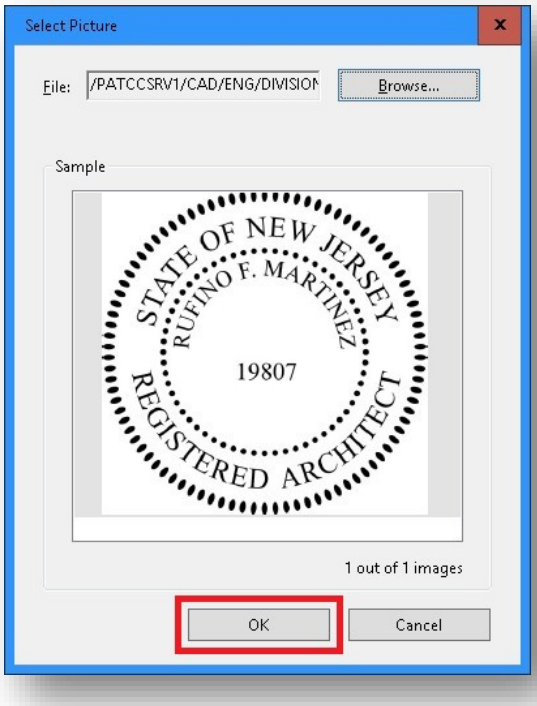




- ‘Select Picture’ pop-up window will appear > Browse…



- Create an appearance for both New York Seal and the New Jersey Seal

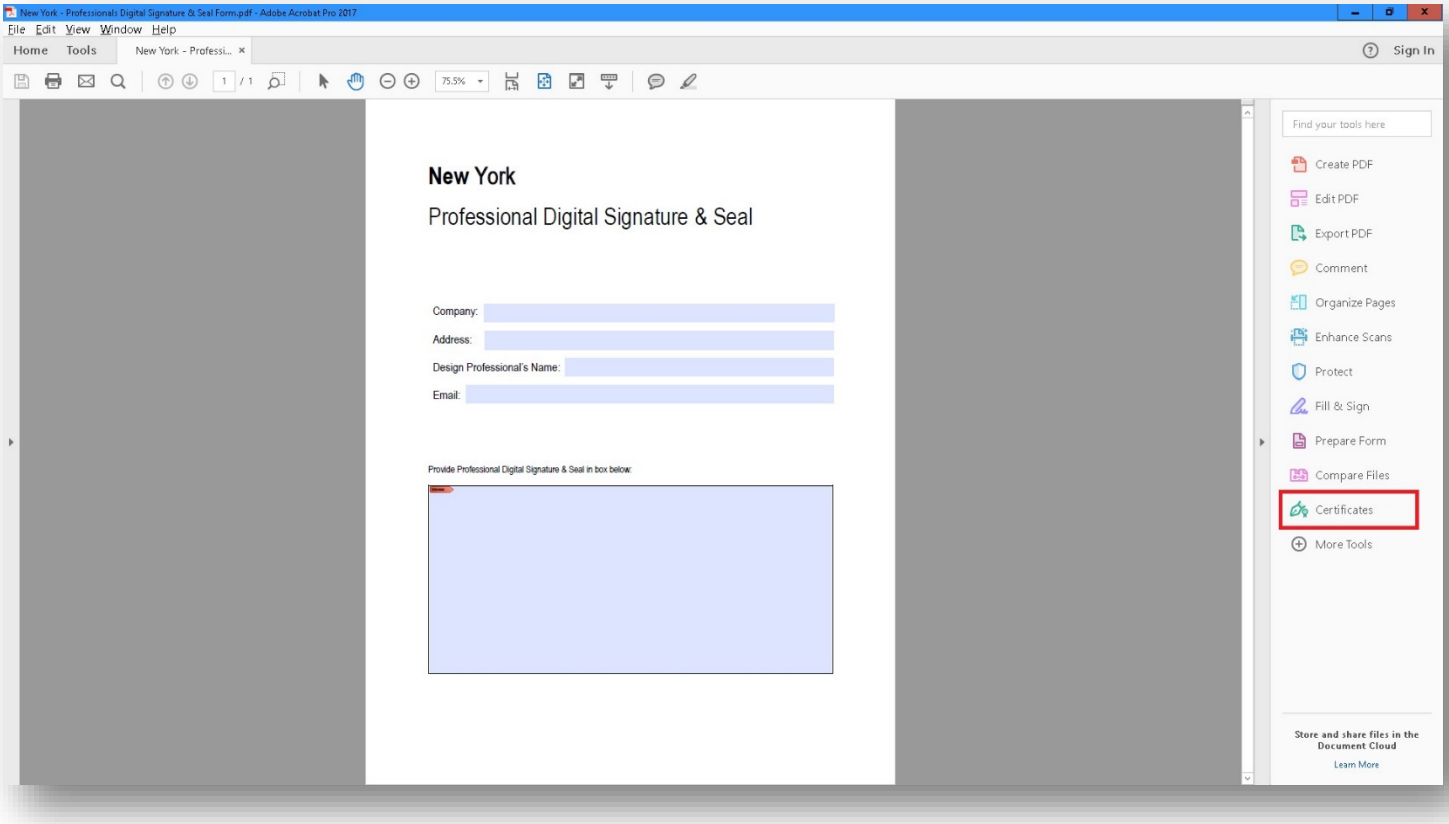


2.7 Setting up your Third-Party Verified Digital Signature

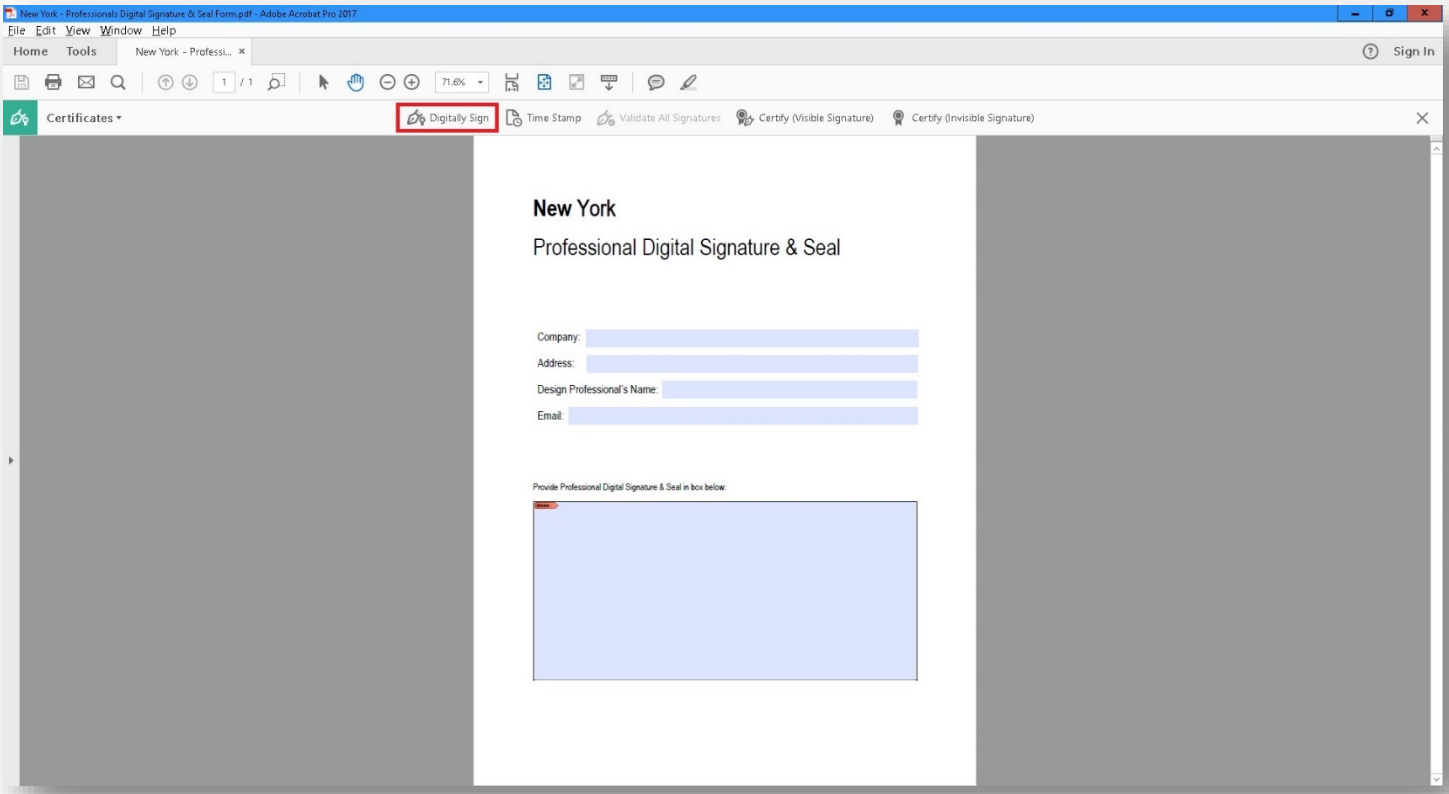
Once you have procured your third-party verified digital signature you need to add this system certificate and private key to your Adobe Acrobat in order for you to digitally sign and seal documents.

Using Adobe Acrobat Standard or Pro.

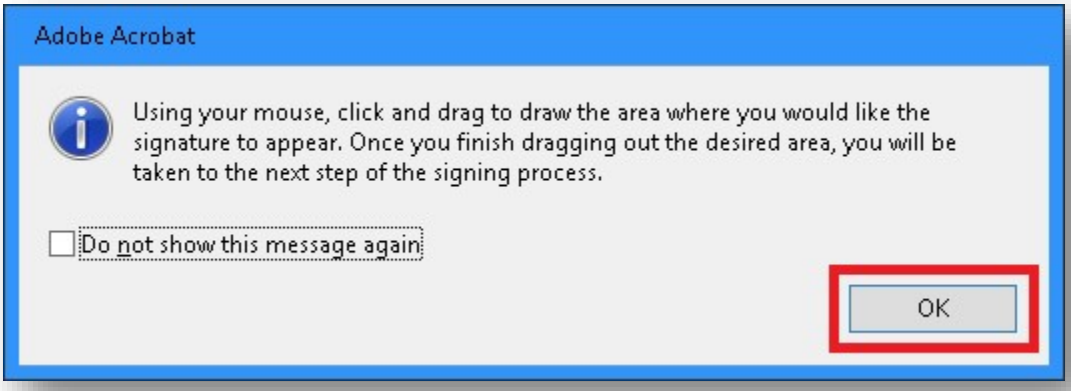
o Open a document that needs to be digitally signed and sealed > Select ‘Certificate’



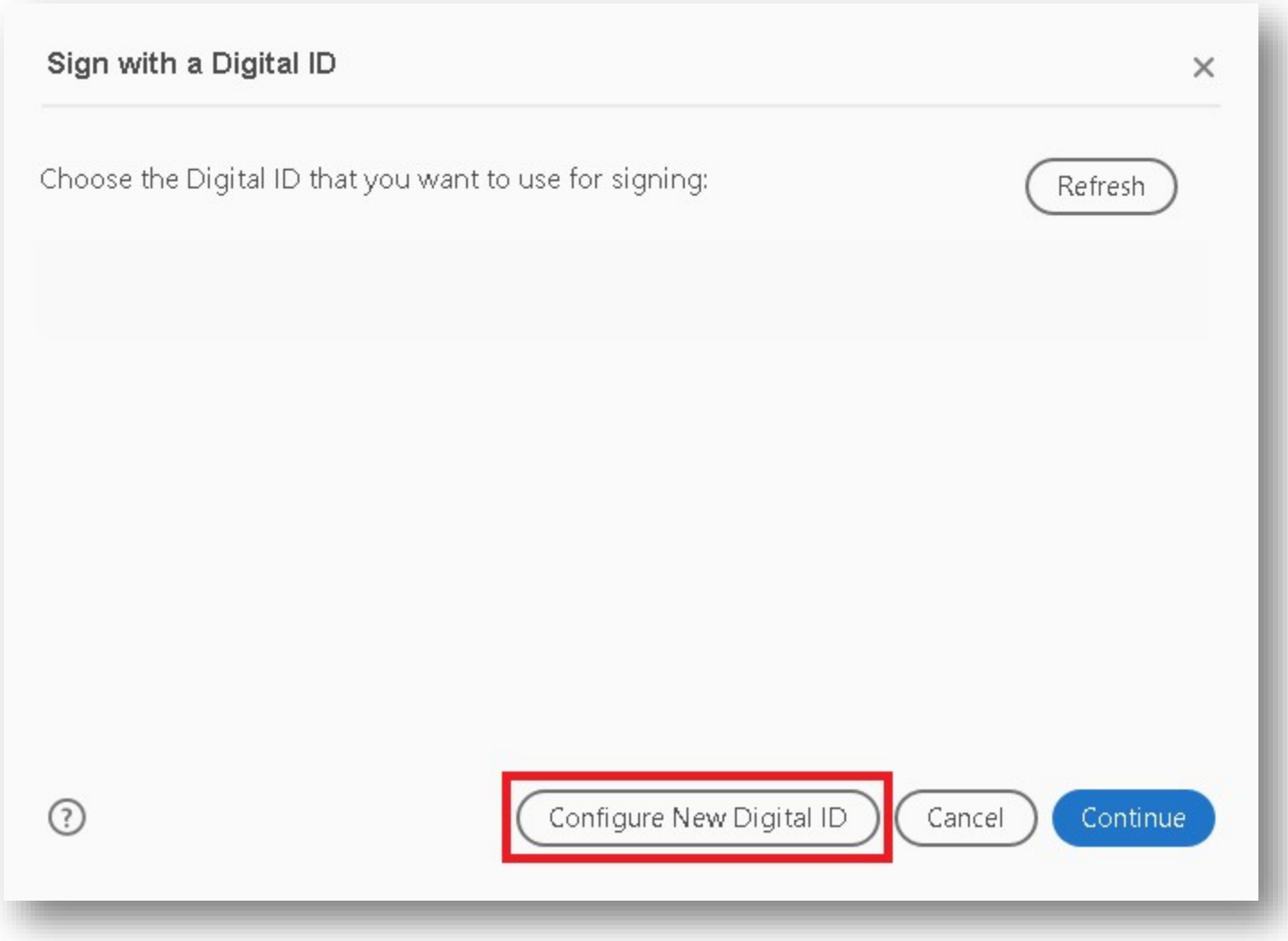
- Select ‘Digitally Sign’



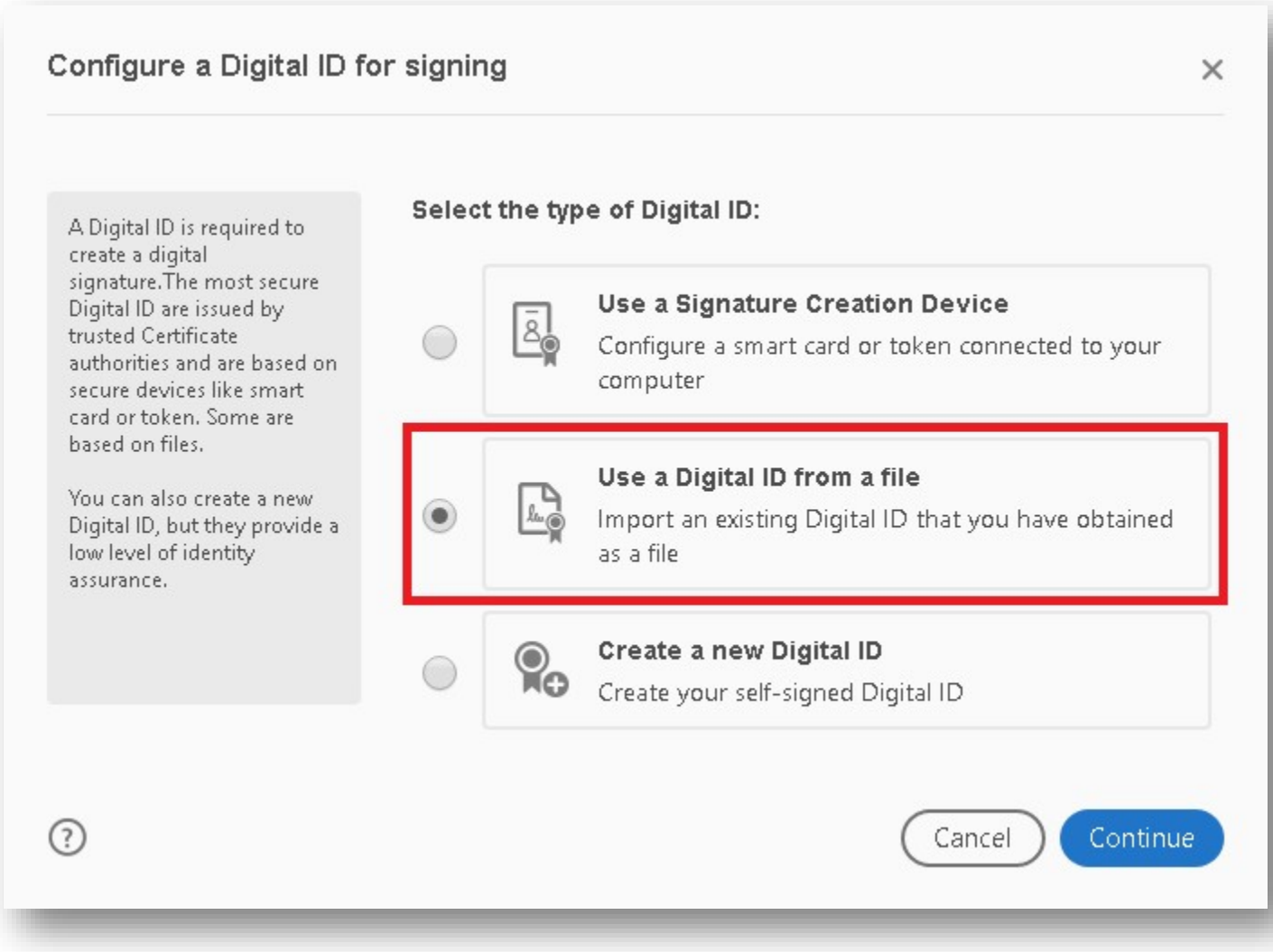
- Select ‘OK’ and Click and drag to draw the area where you would like the signature to appear on the document.



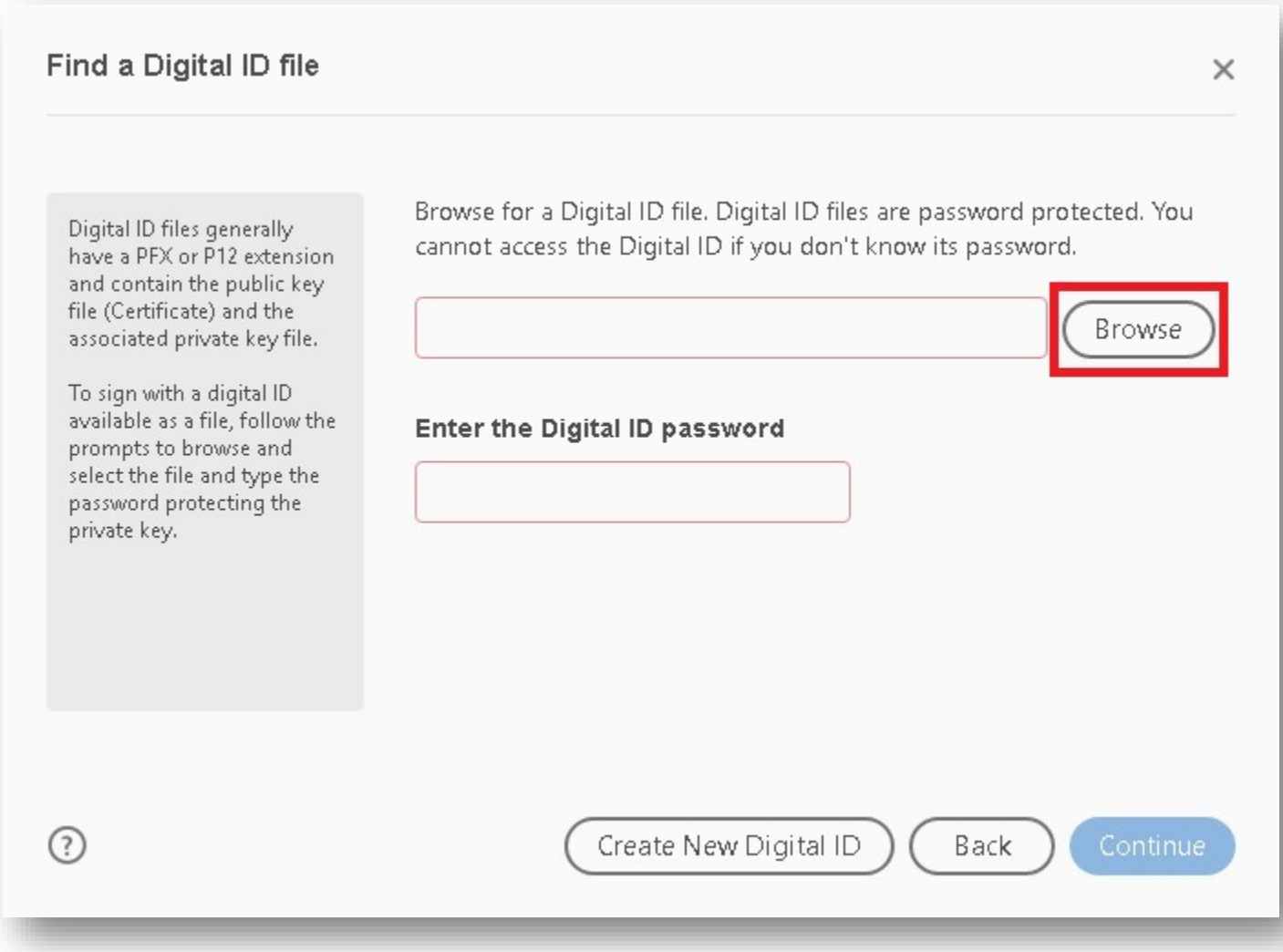
- Once the area is selected, a ‘Sign with a Digital ID’ pop-up window will appear. Select ‘Configure New Digital ID’



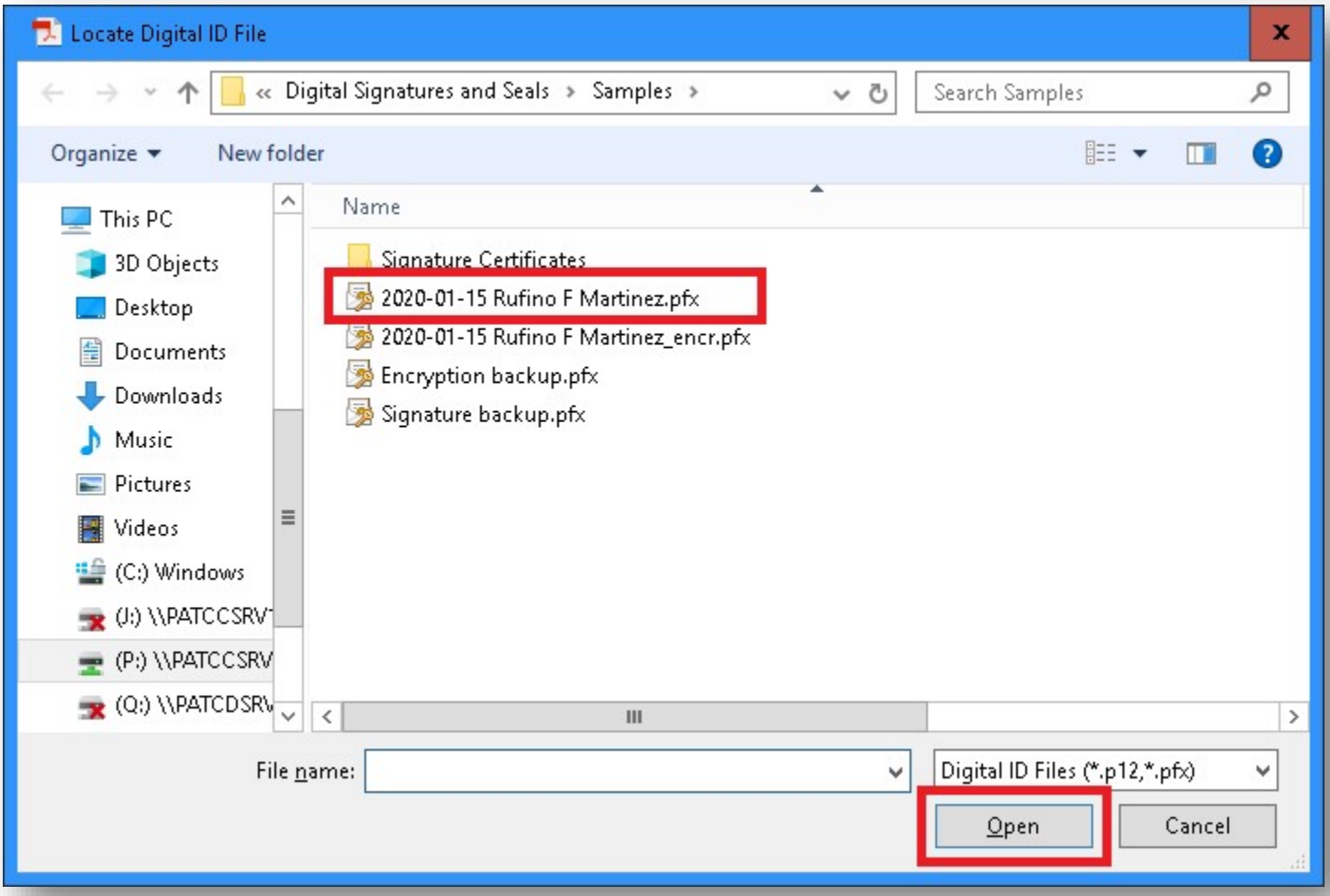
o ‘Configure a Digital ID for signing’ will appear. > Select ‘Use a Digital ID from a file’ > Continue



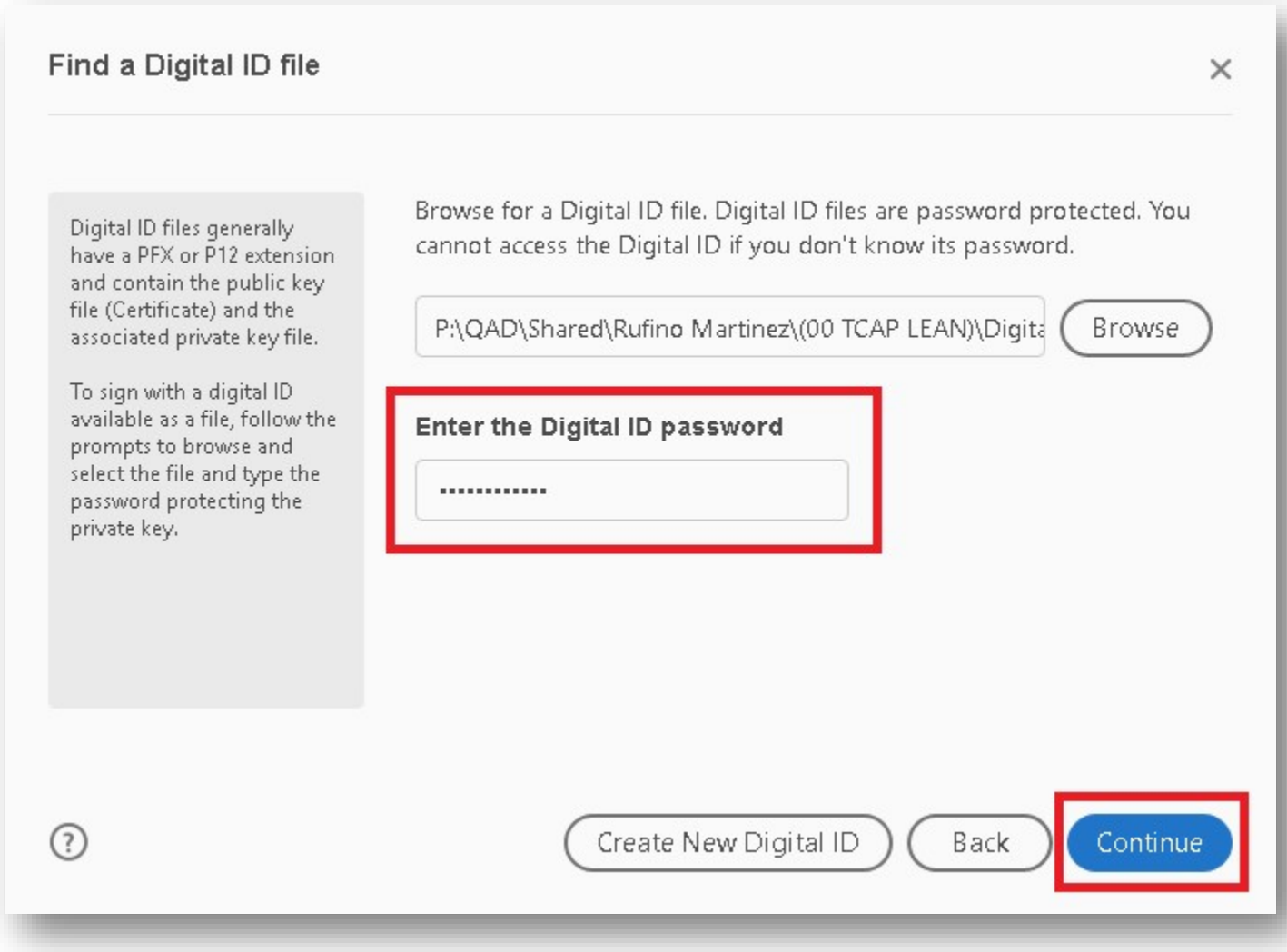
o ‘Find a Digital ID file ’pop-up window will appear. Select ‘Browse’



o ‘Locate your digital ID File’ will appear. *(.pfx file is a single, password protected certificate archive that contains the entire certificate chain plus the matching private key.)*

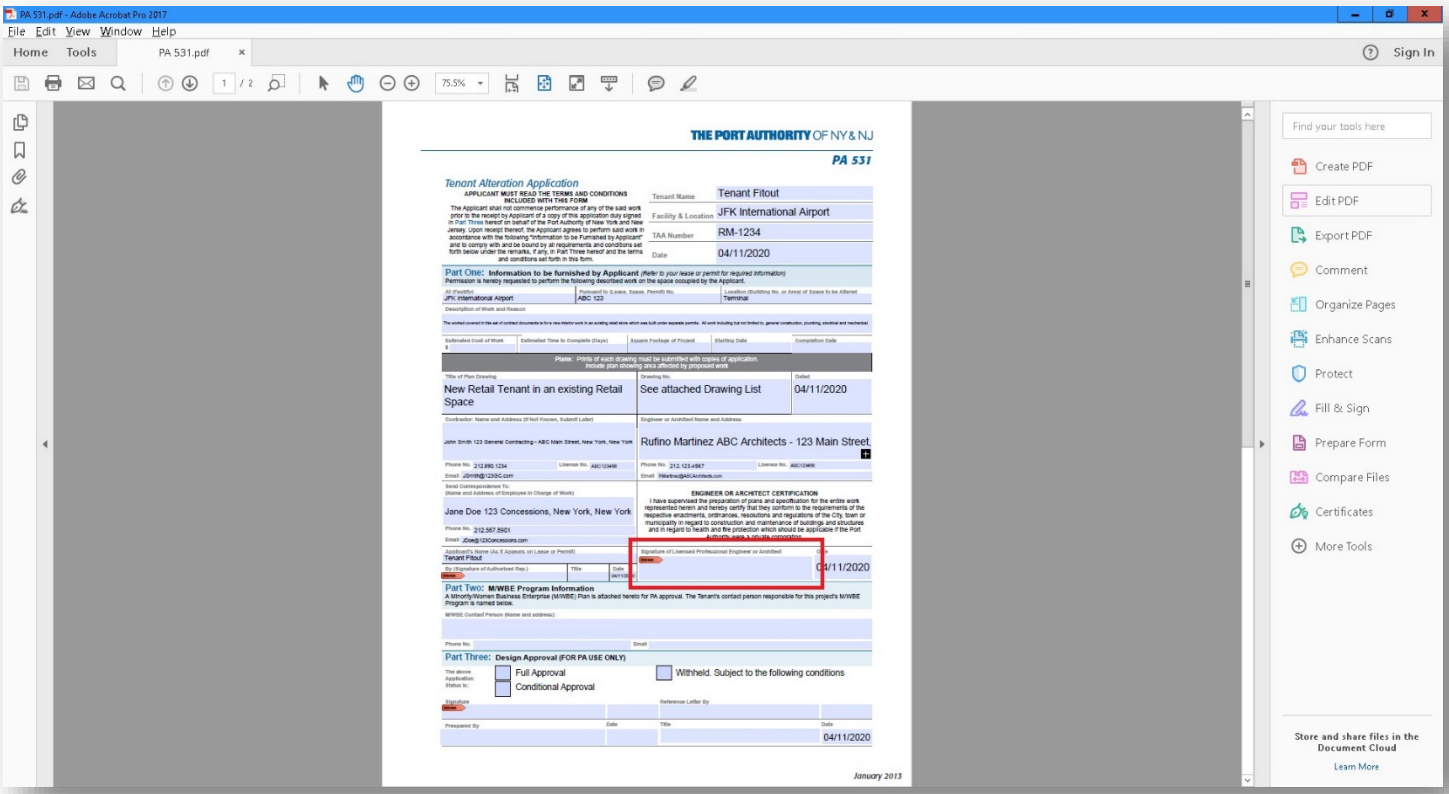


o Find a Digital ID file 'pop-up window will appear. Enter the Digital ID password > Continue

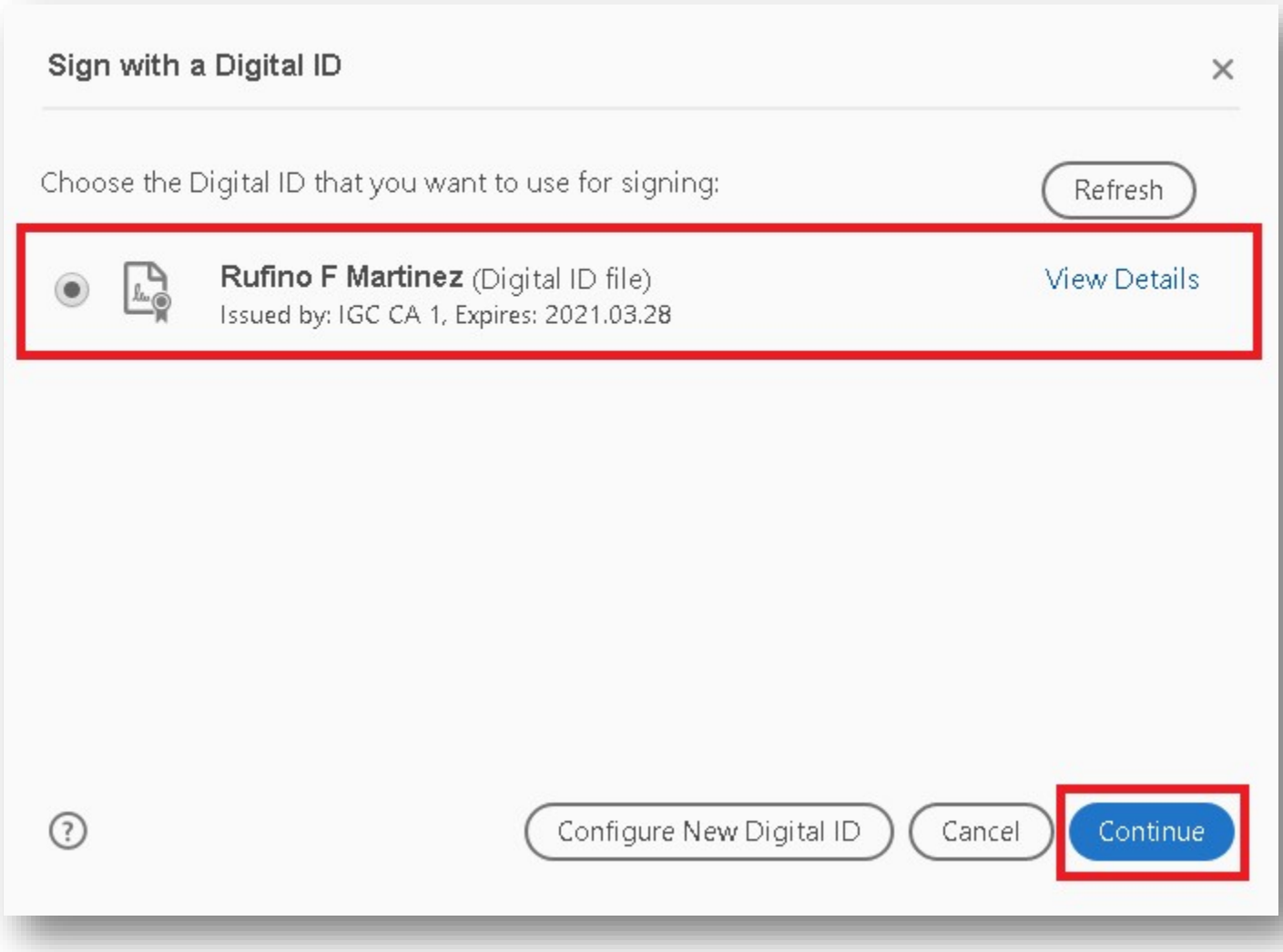


2.8 How to Apply your Digital Signature

o Open the document that needs to be Digitally Signed. Select the area that needs to be signed.



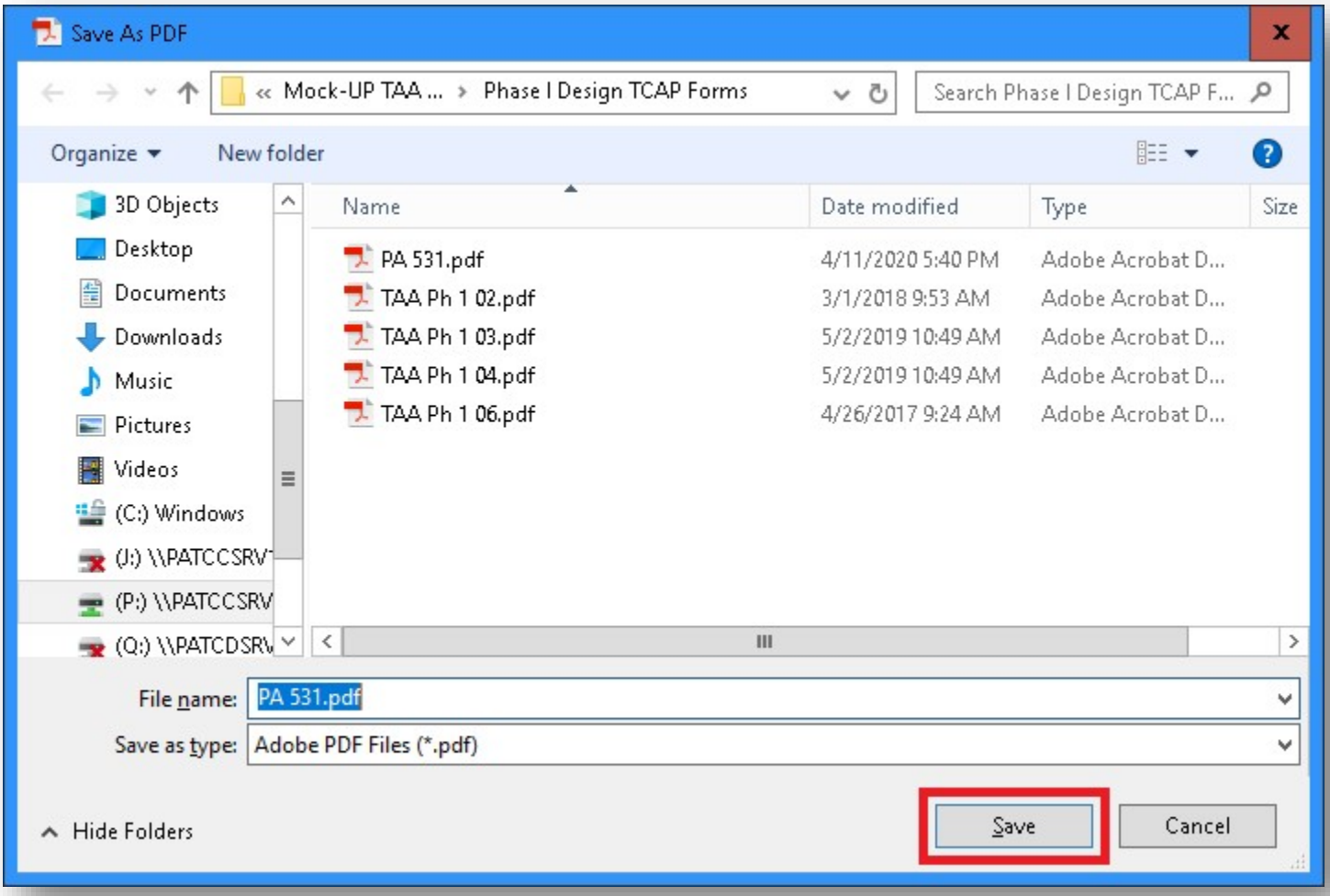
o ‘Sign with a Digital ID’ pop-up window will appear. Choose your ‘Digital ID file’ > Continue



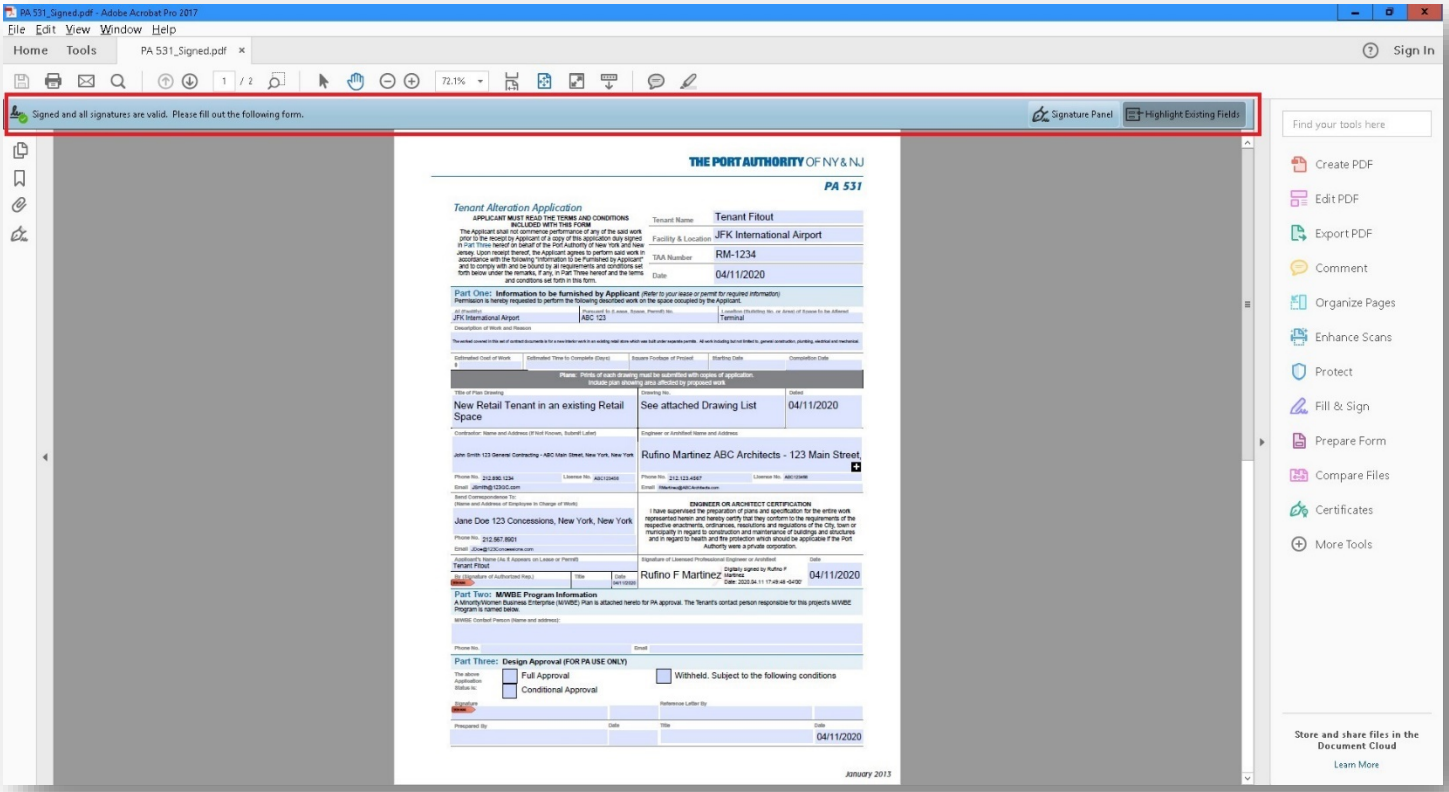
o ‘Sign as Rufino F Martinez’ pop-up window will appear > Appearance > Scroll down to Standard Text

o ‘Sign as Rufino F Martinez’ pop-up window will appear > Enter the Digital ID PIN or Password…>Sign

o ‘Save As PDF’ pop-up window will appear > Save

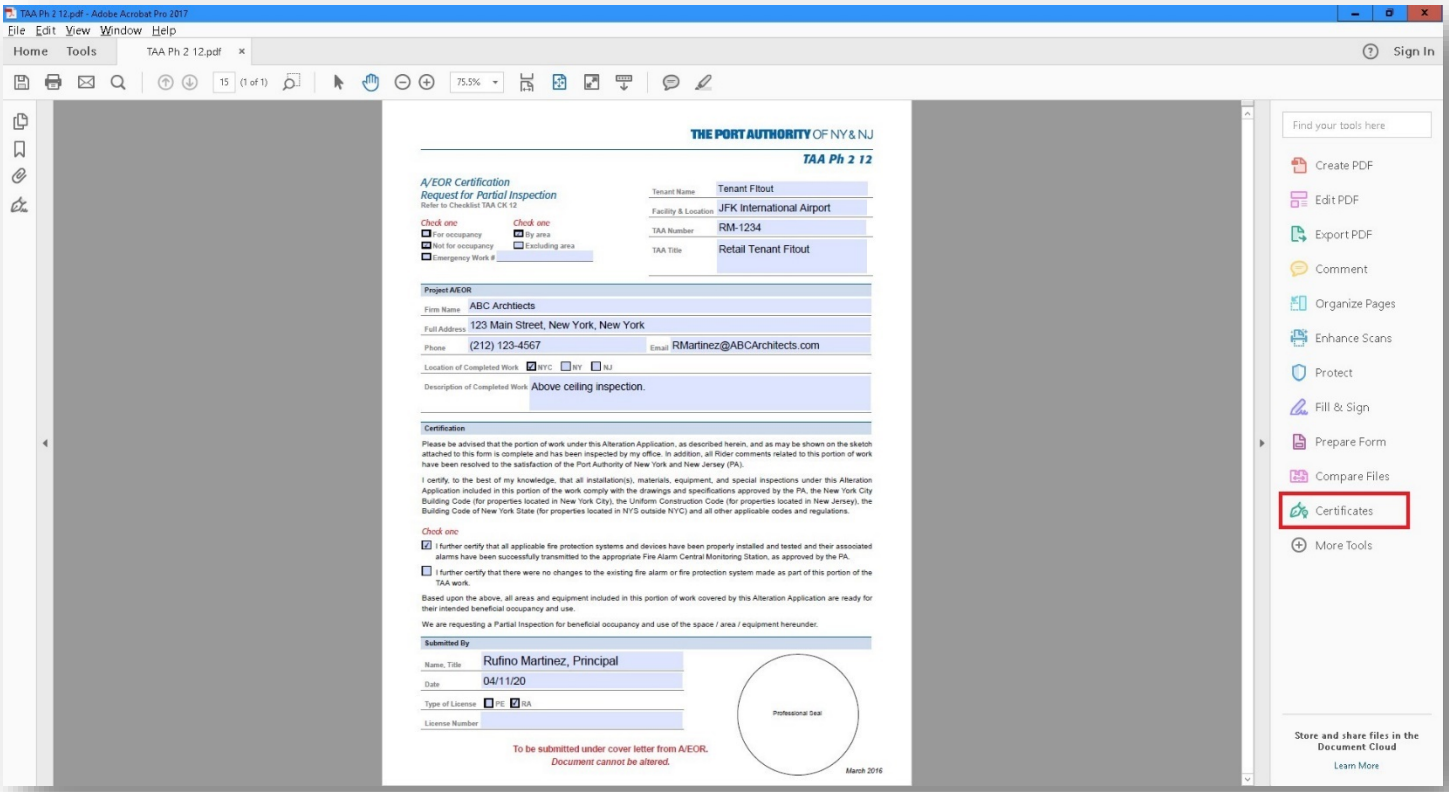


- Once the document is saved you will notice the blue ribbon across the top of the document to indicate the document has been digitally signed.

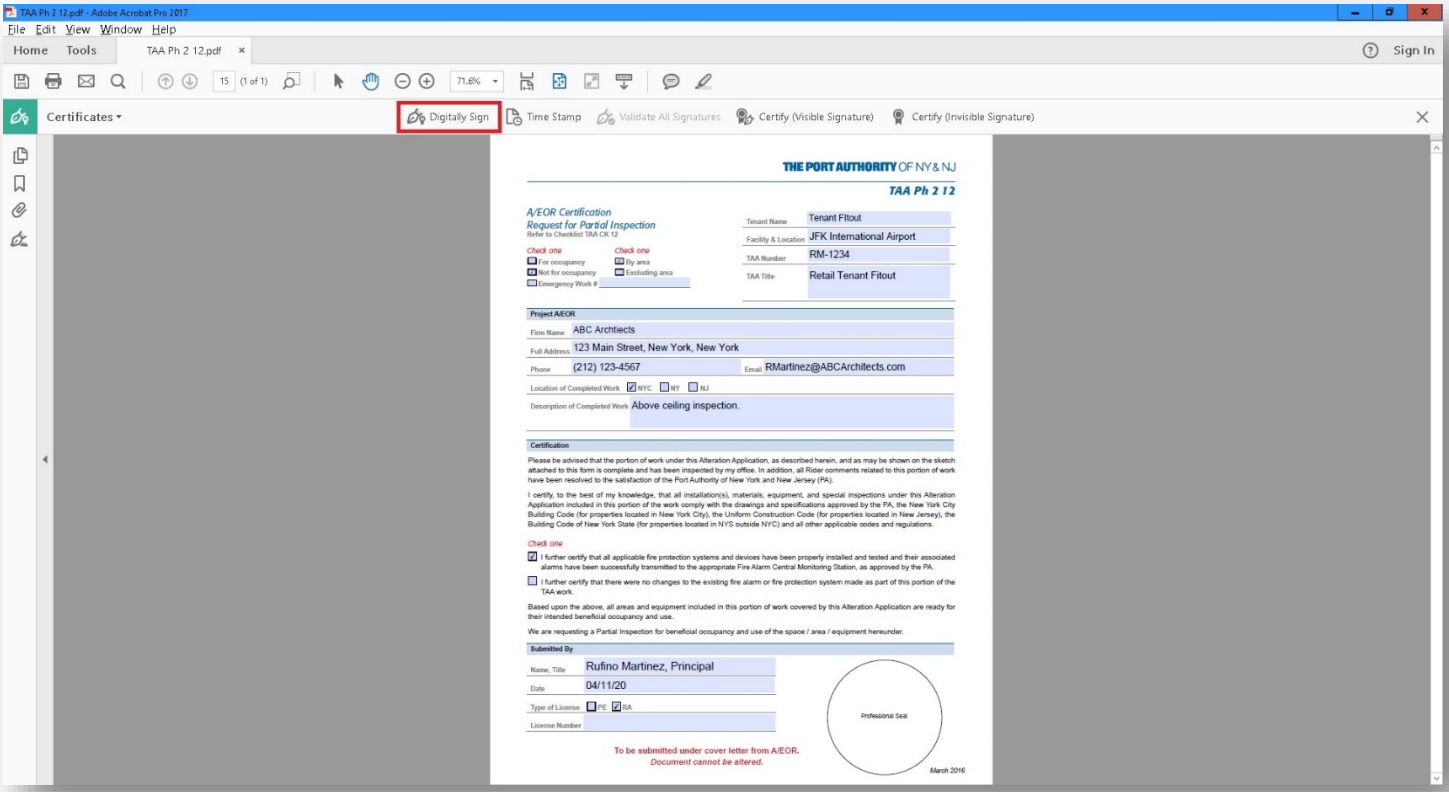


2.9 How to Apply your Digital Signature & Seal

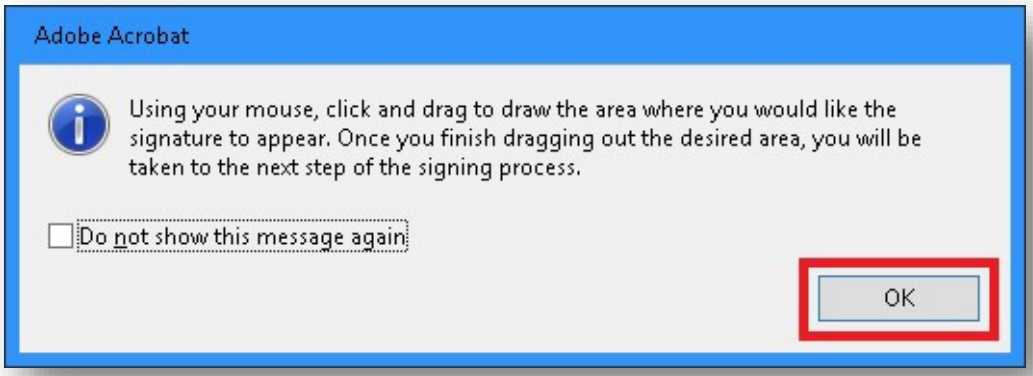
o Open the document that needs to be Digitally Signed & Sealed. > Select ‘Certificates’



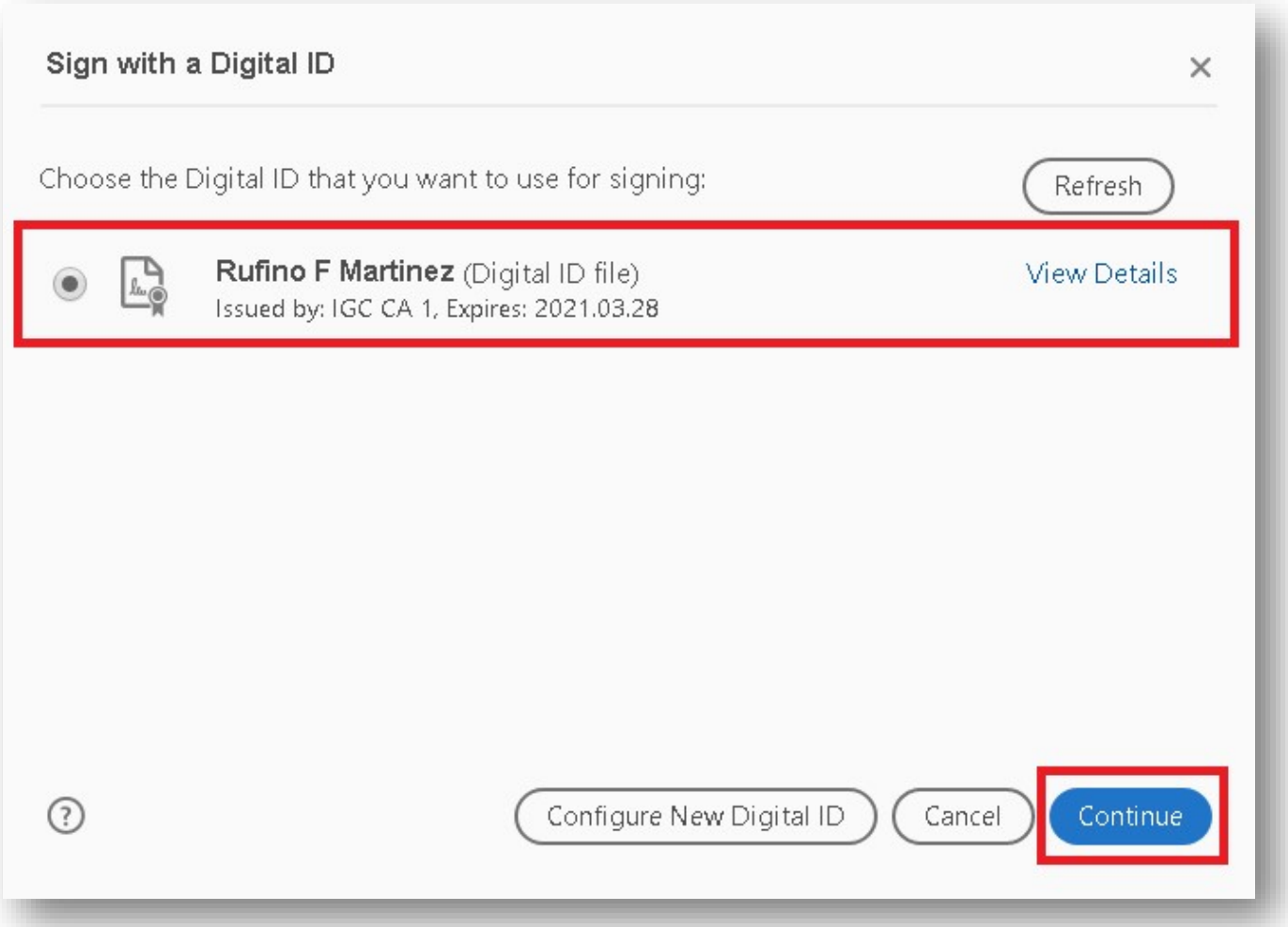
o Select ‘Digitally Sign’



- Select ‘OK’ and Click and drag to draw the area where you would like the signature and seal to appear on the document.



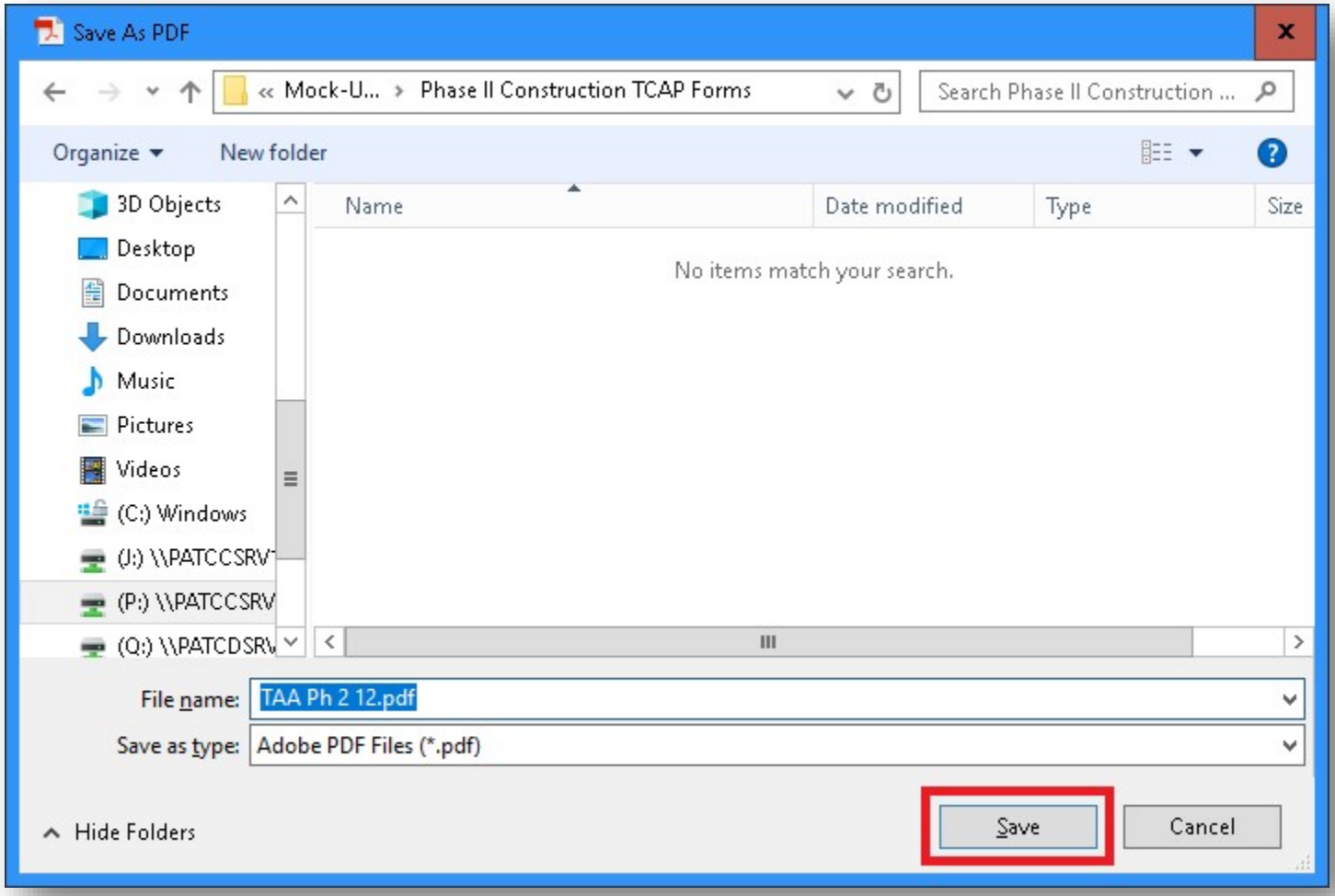
- ‘Sign with a Digital ID’ pop-up window will appear. Choose your ‘Digital ID file’ > Continue



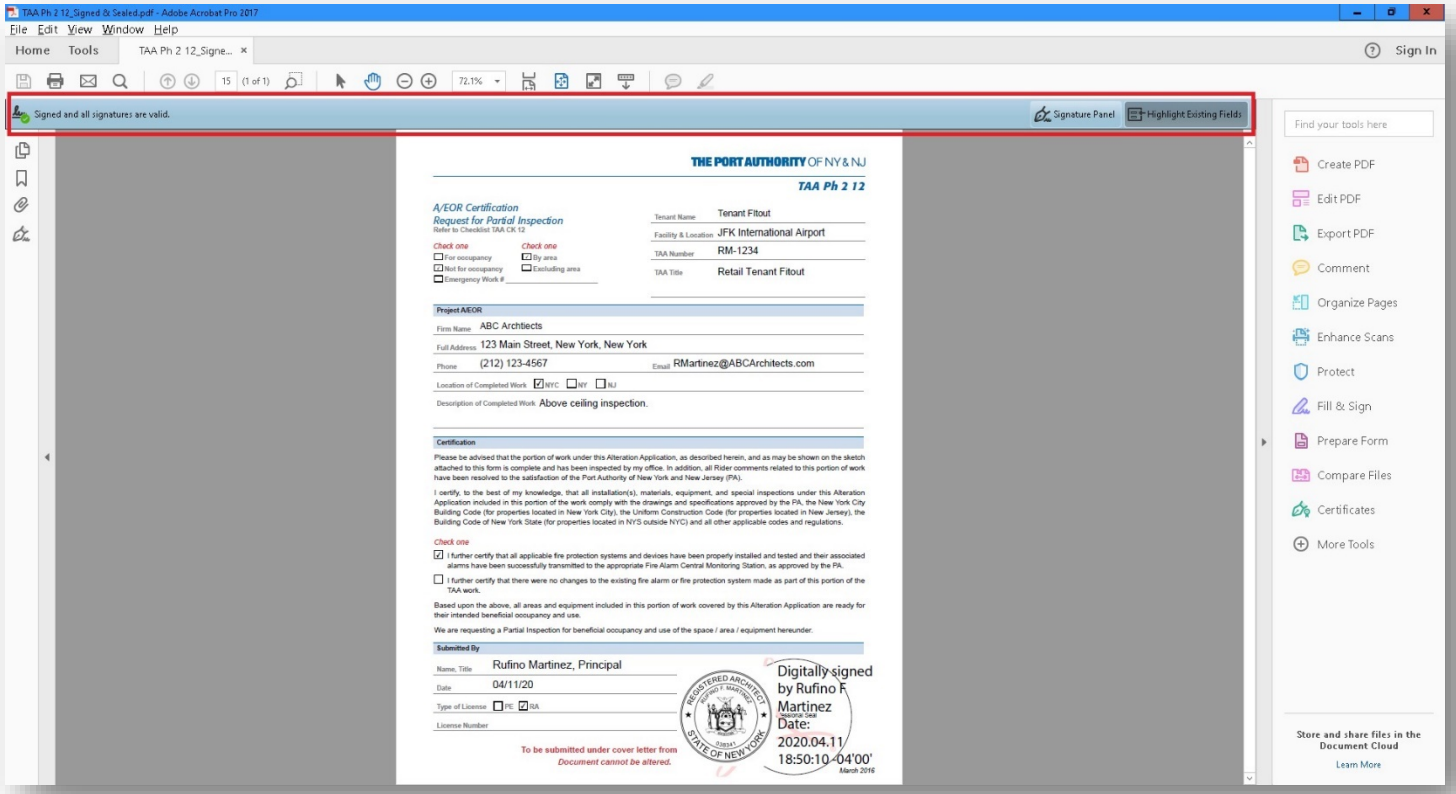
o ‘Sign as Rufino F Martinez’ pop-up window will appear > Appearance > Scroll down to select the appropriate state seal ‘New York Seal’

- ‘Sign as Rufino F Martinez’ pop-up window will appear > Select ‘Lock document after signing’ > Enter the Digital ID PIN or Password…>Sign

o ‘Save As PDF’ pop-up window will appear > Save

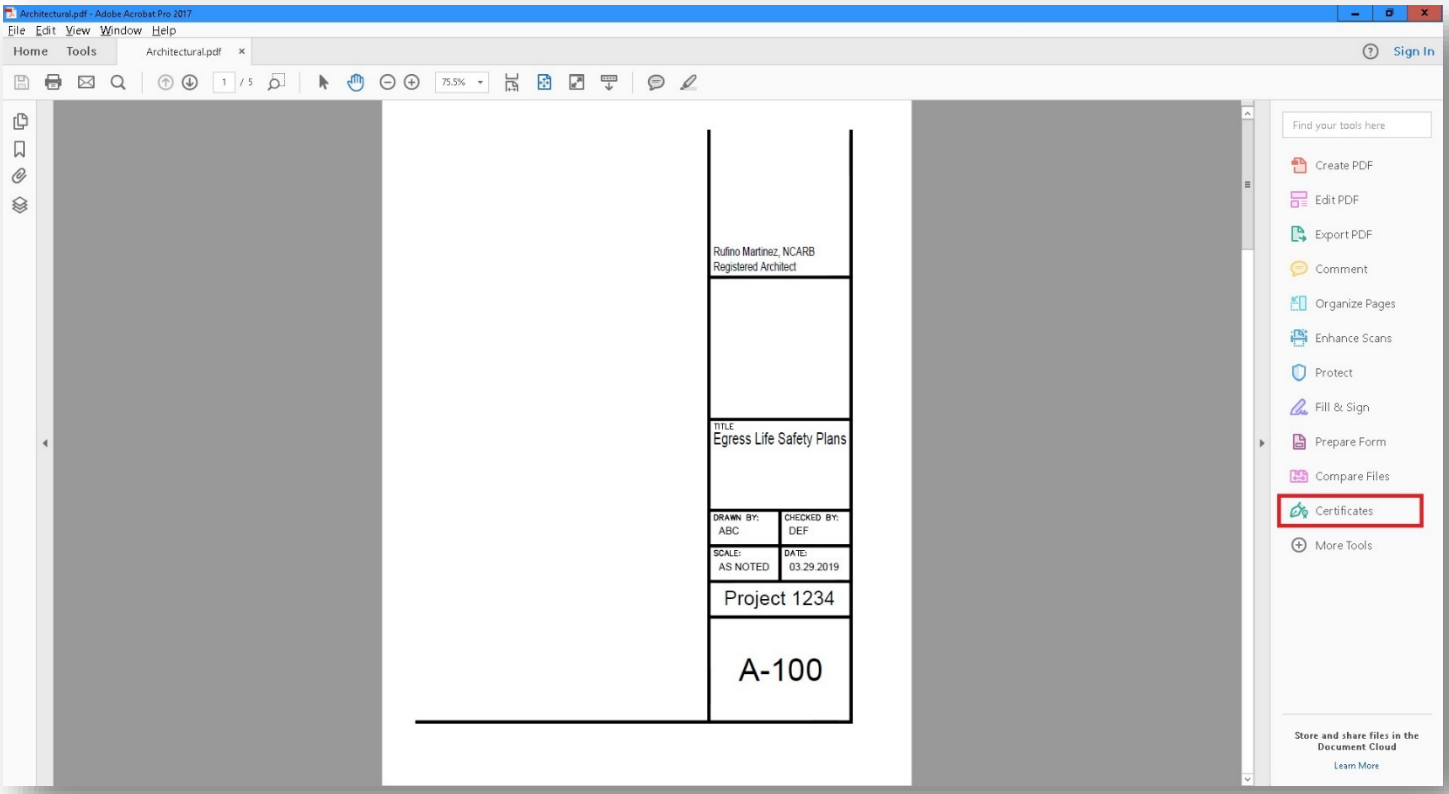


- Once the document is saved you will notice the blue ribbon across the top of the document to indicate the document has been digitally signed.

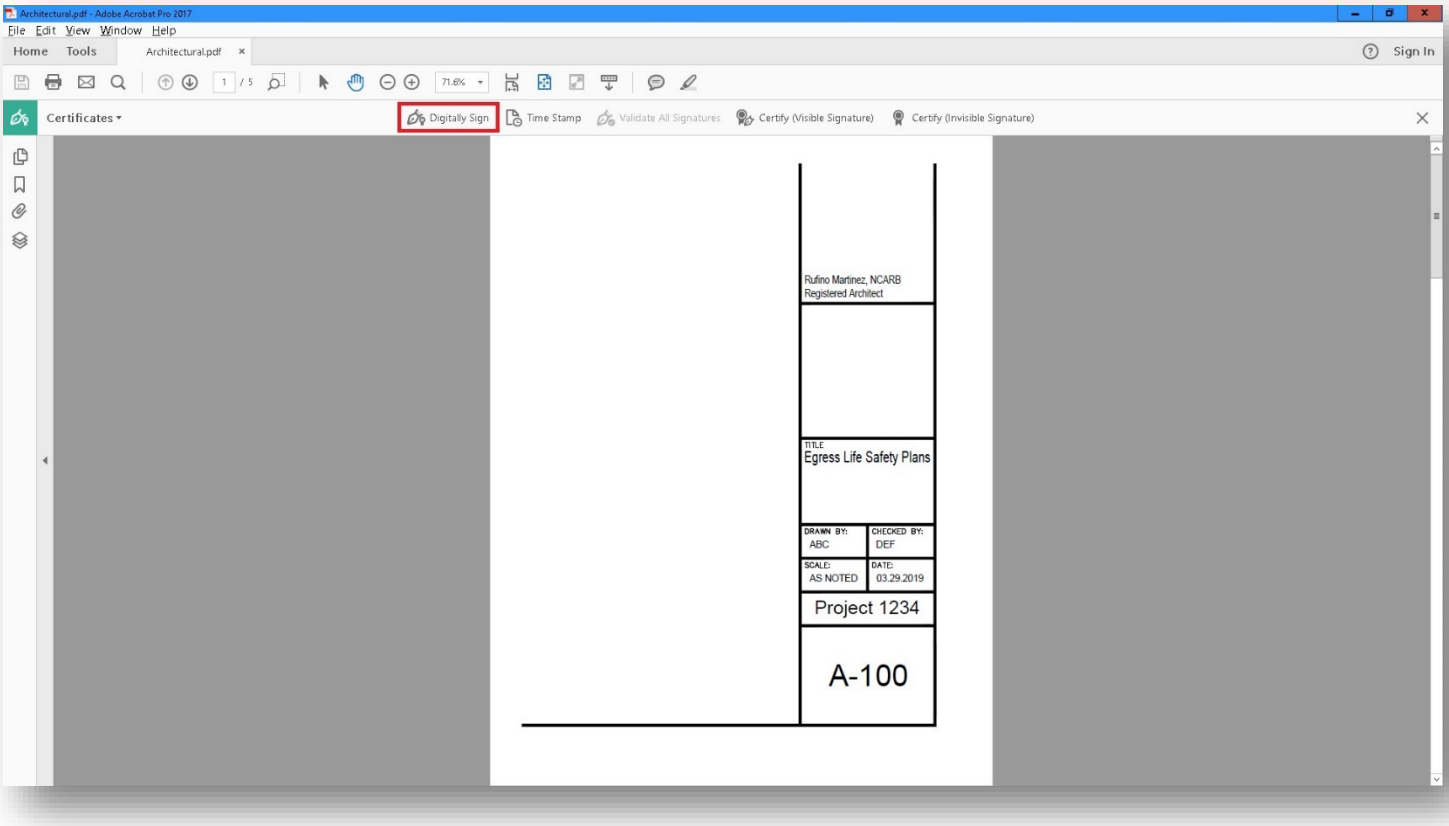


2.10 How to Apply your Digital Signature & Seal on Multi-page Documents

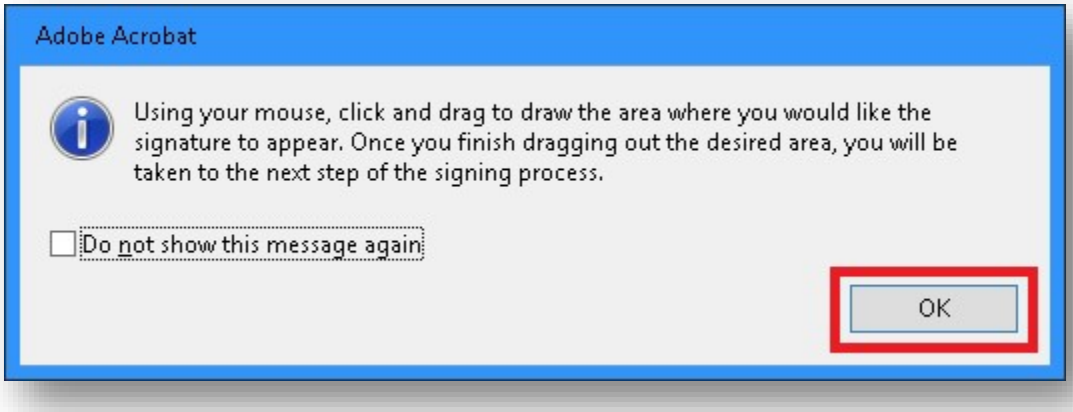
o Open the multi-page document that needs to be Digitally Signed & Sealed. > Select 'Certificates'



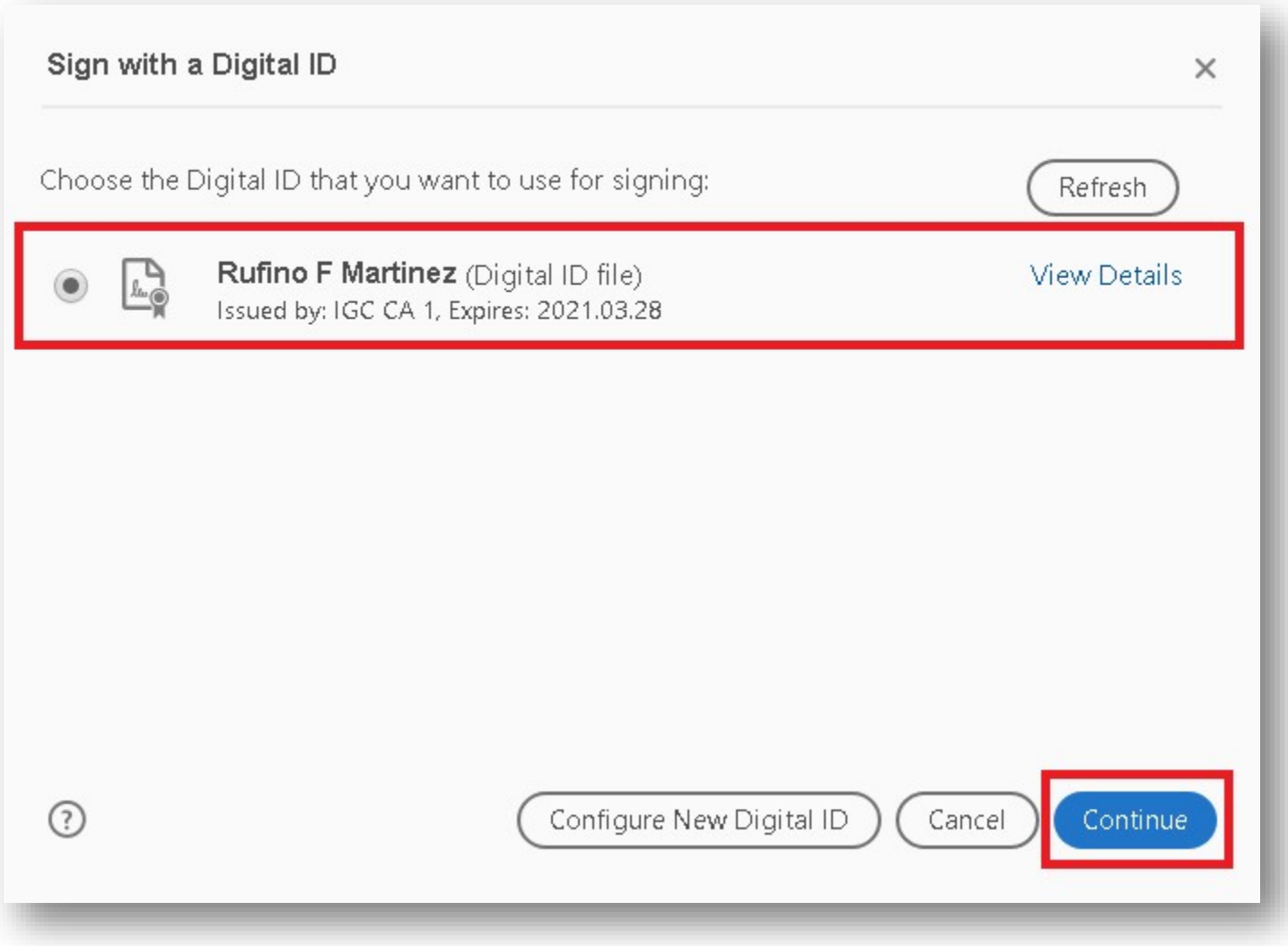
- Select ‘Digitally Sign’



- Select ‘OK’ and Click and drag to draw the area where you would like the signature and seal to appear on the document.



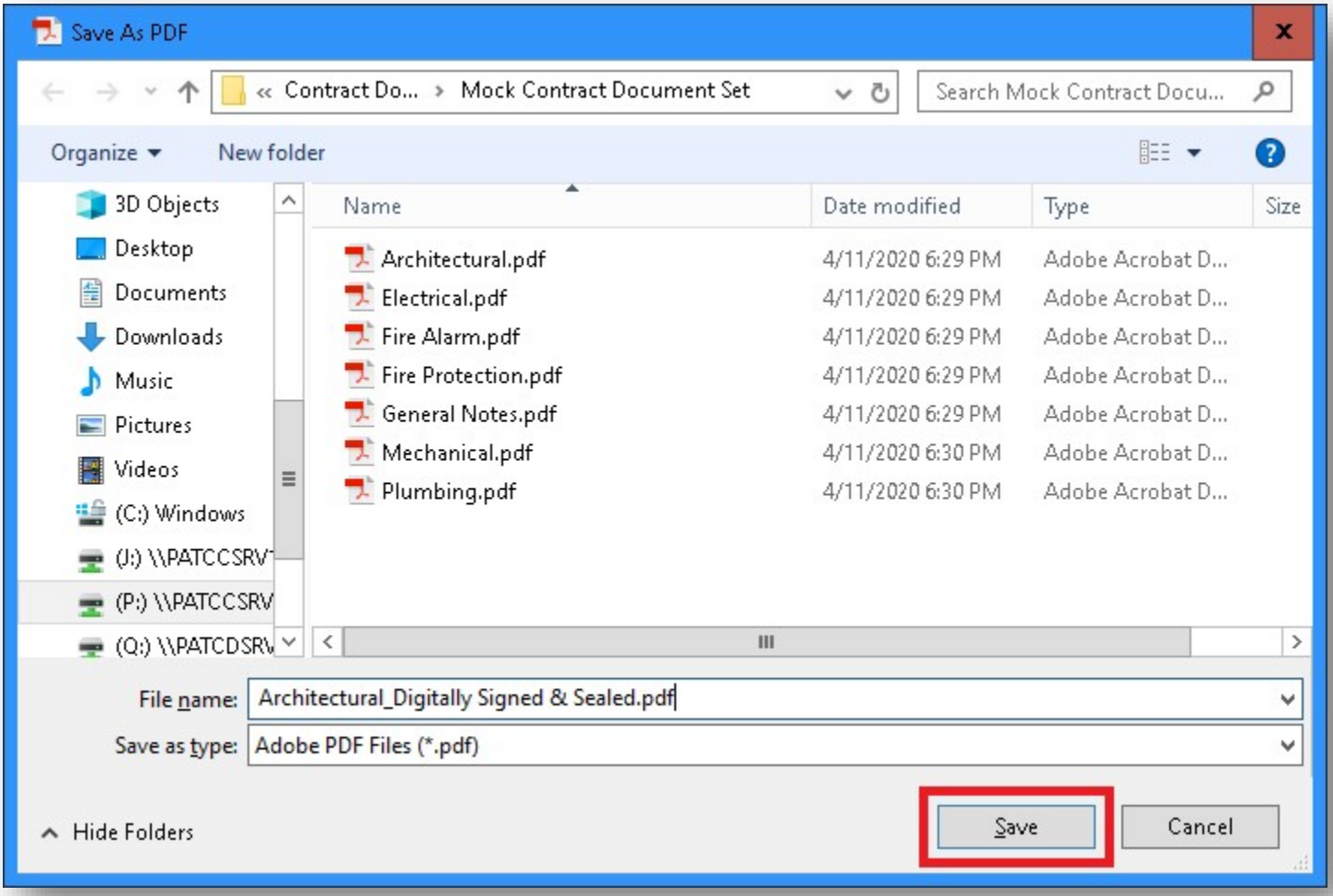
o ‘Sign with a Digital ID’ pop-up window will appear > Choose your ‘Digital ID file’ > Continue



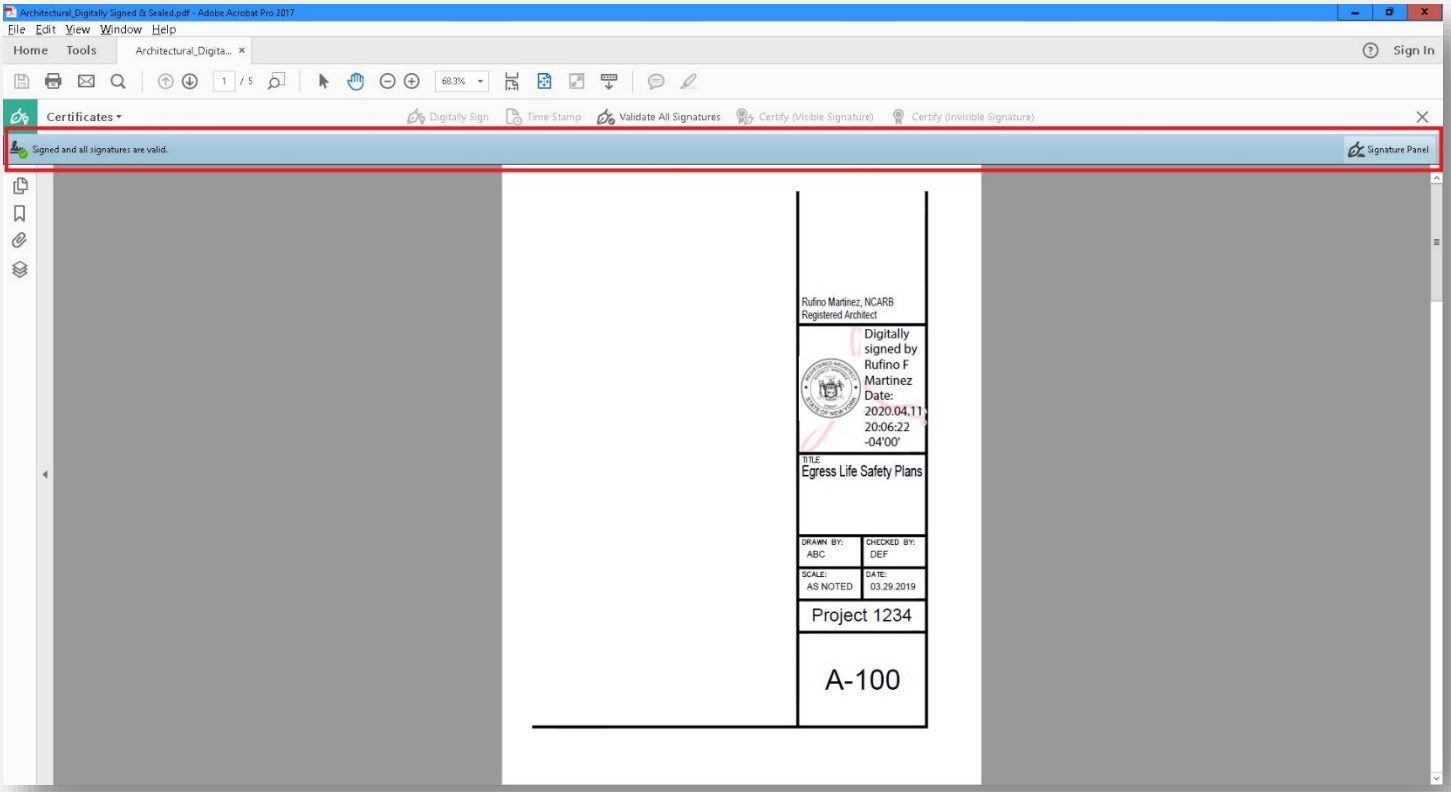
- ‘Sign as “Rufino F Martinez”’ pop-up window will appear > Appearance > Scroll down to select the appropriate state seal ‘New York Seal’

o ‘Sign as Rufino F Martinez’ pop-up window will appear > **DO NOT SELECT** ‘Lock document after signing’ > Enter the Digital ID PIN or Password…>Sign

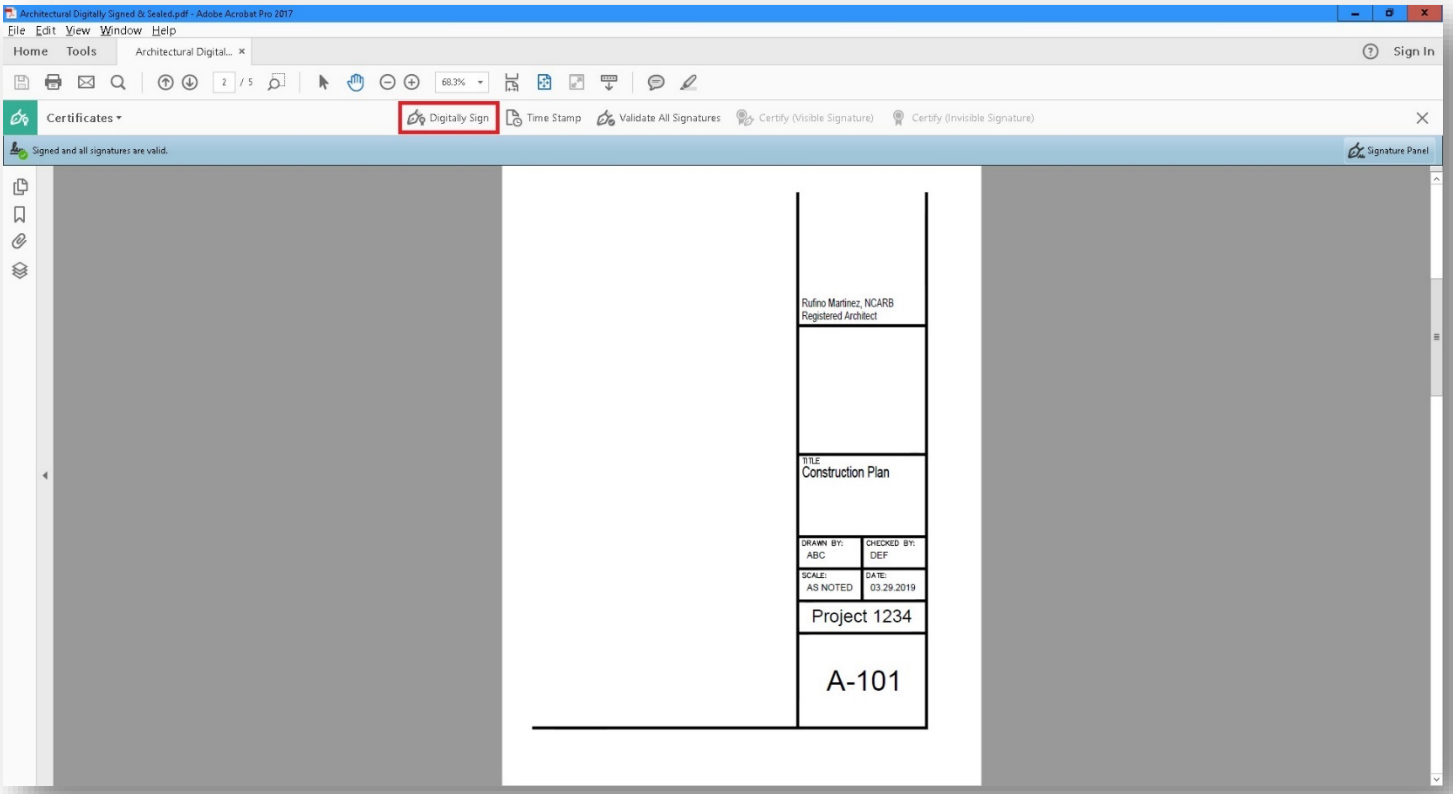
o ‘Save As PDF’ pop-up window will appear > Save



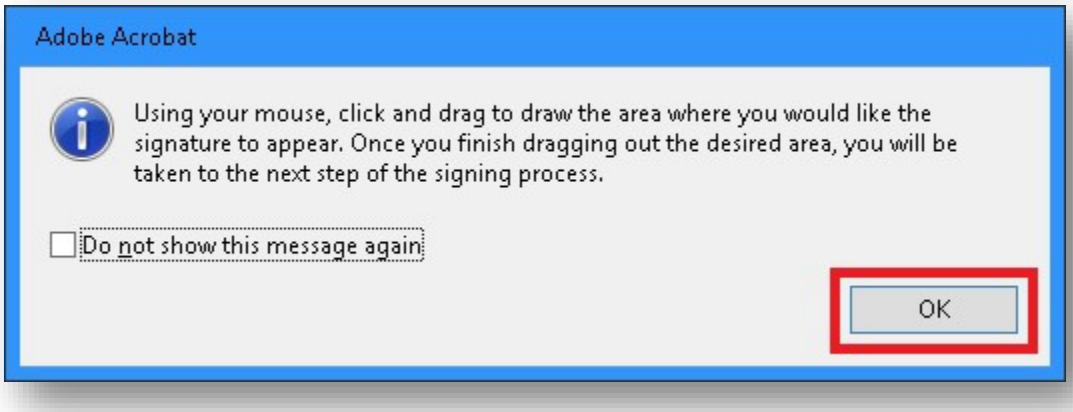
- Once the document is saved you will notice the blue ribbon across the top of the document to indicate the first document of the multi-page document has been digitally signed and sealed.



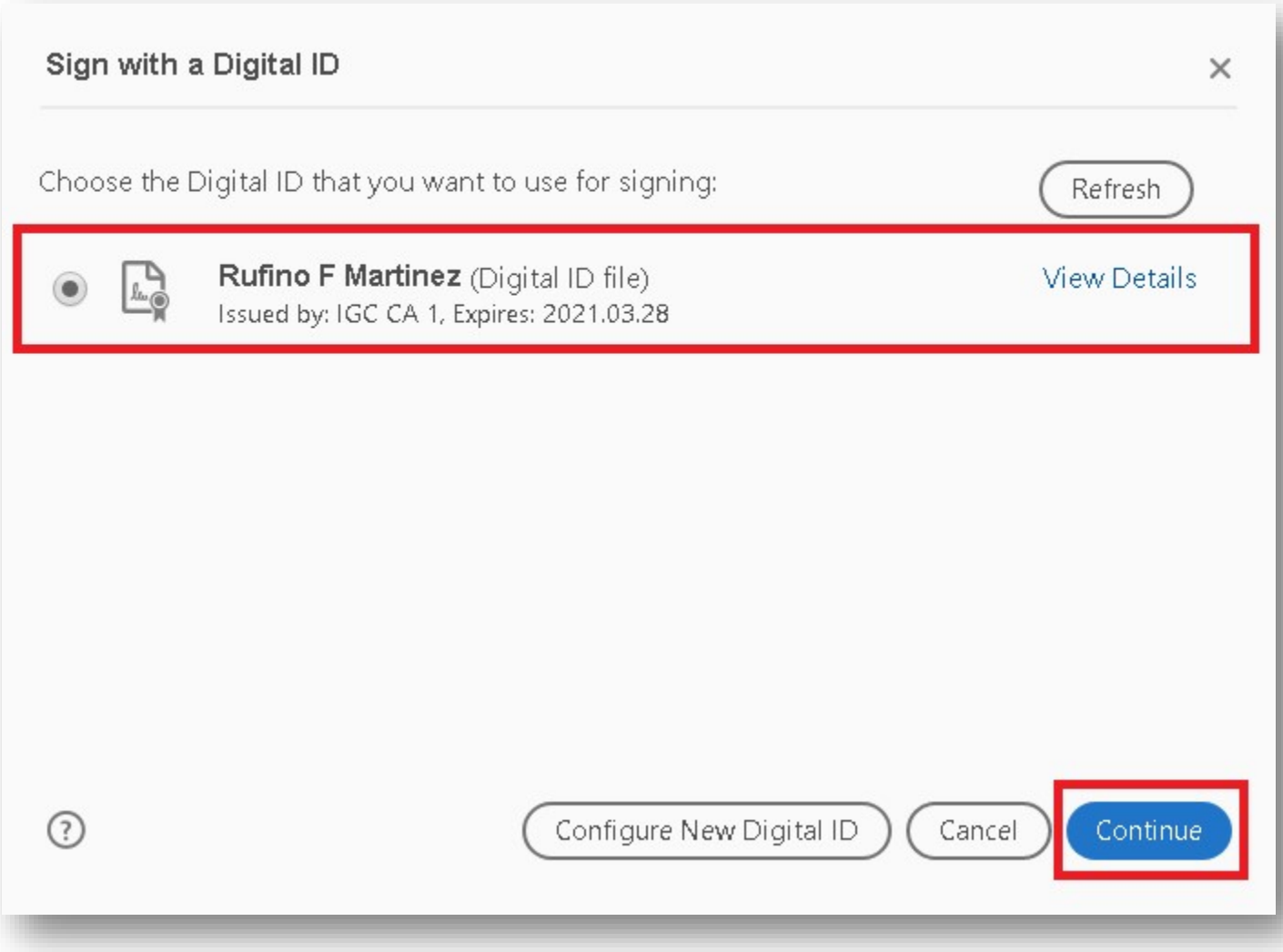
- Scroll down to the next page select ‘Digitally Sign’



- Select ‘OK’ and Click and drag to draw the area where you would like the signature and seal to appear on the document.



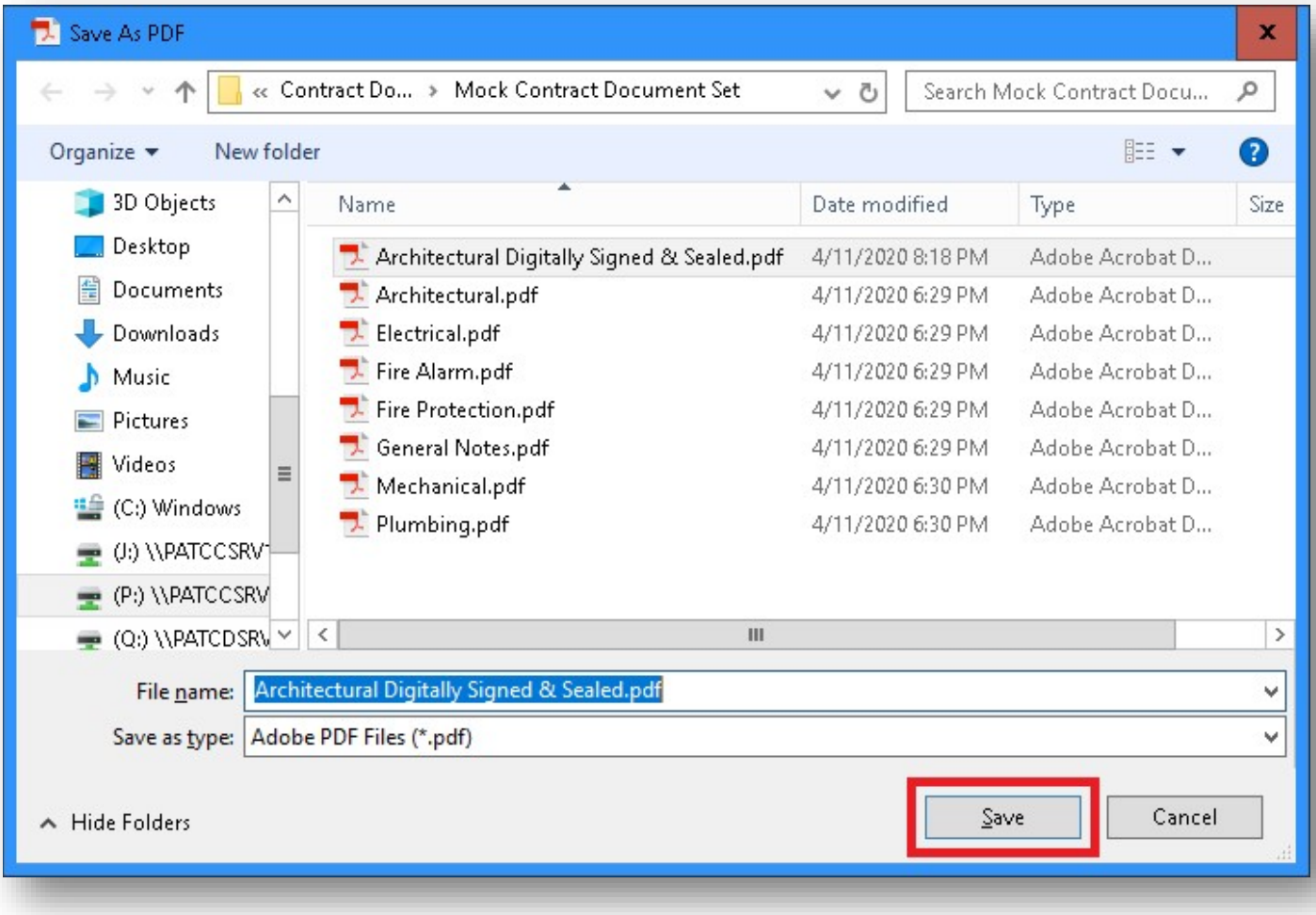
o ‘Sign with a Digital ID’ pop-up window will appear > Choose your ‘Digital ID file’ > Continue



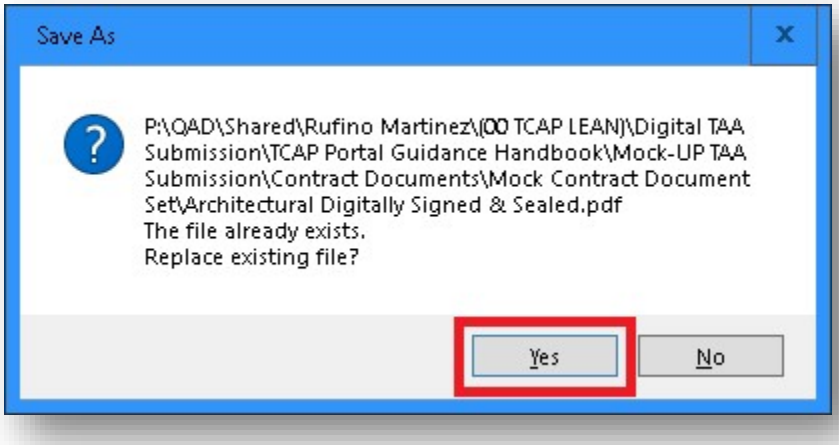
- Sign as Rufino F Martinez' pop-up window will appear > Appearance > Scroll down to select the appropriate state seal 'New York Seal'

- ‘Sign as Rufino F Martinez’ pop-up window will appear > **DO NOT SELECT** ‘Lock document after signing’ > Enter the Digital ID PIN or Password…>Sign

- ‘Save As PDF’ pop-up window will appear > Save over the previous file



- ‘Save As’ pop-up window will appear > ‘…Replace existing file?’ > Yes

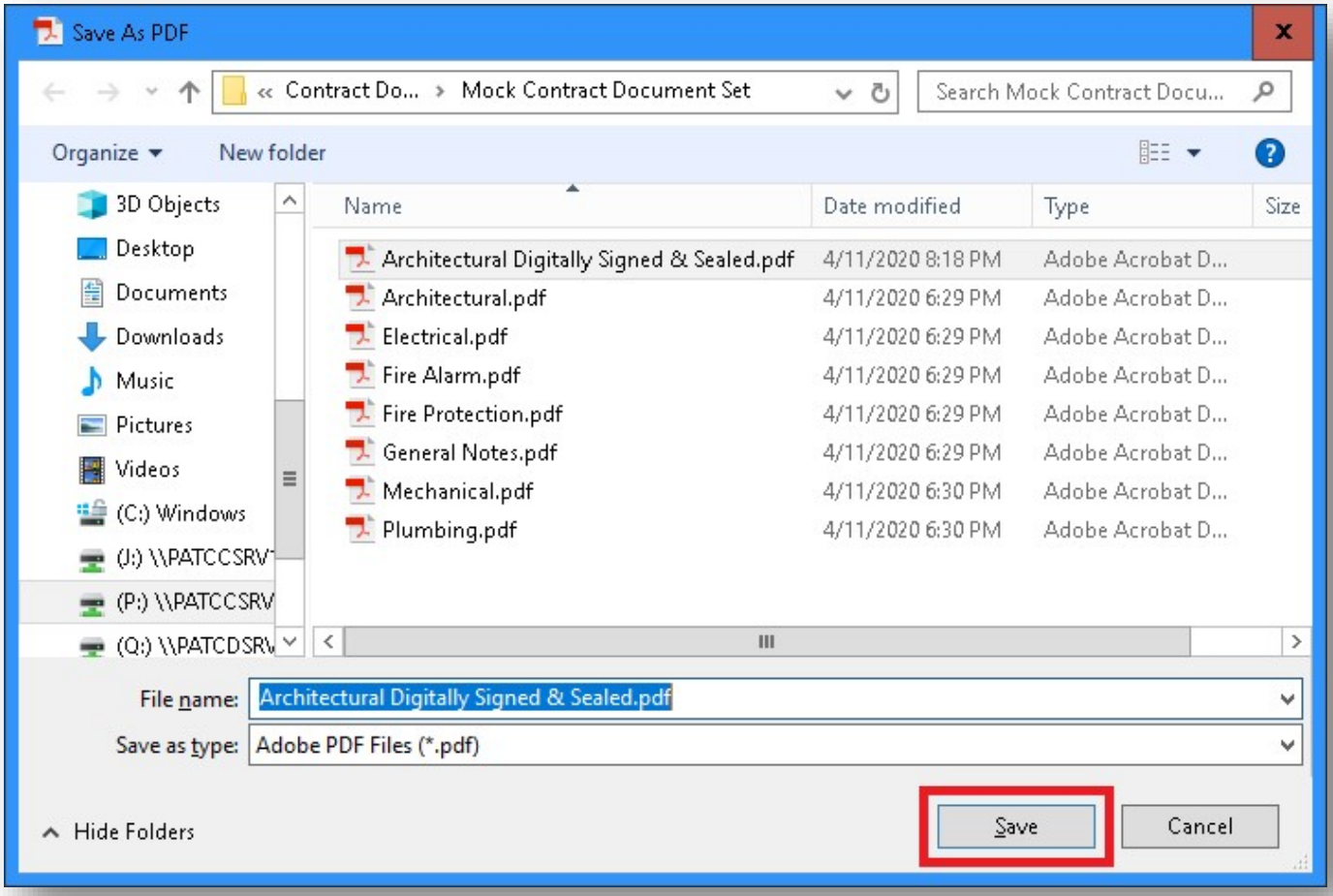


This process will be repeated until all documents have been digitally signed & sealed within the multi-page document.

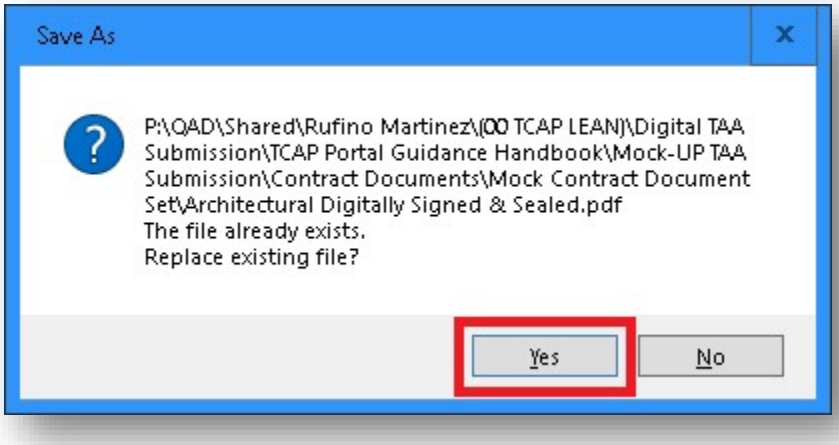
IMPORTANT
When digitally signing and sealing the **last page of the multi-page document** you will need to '**lock the document after signing'.**

o 'Sign as Rufino F Martinez' pop-up window will appear > **Select 'Lock document after signing'** > Enter the Digital ID PIN or Password…>Sign

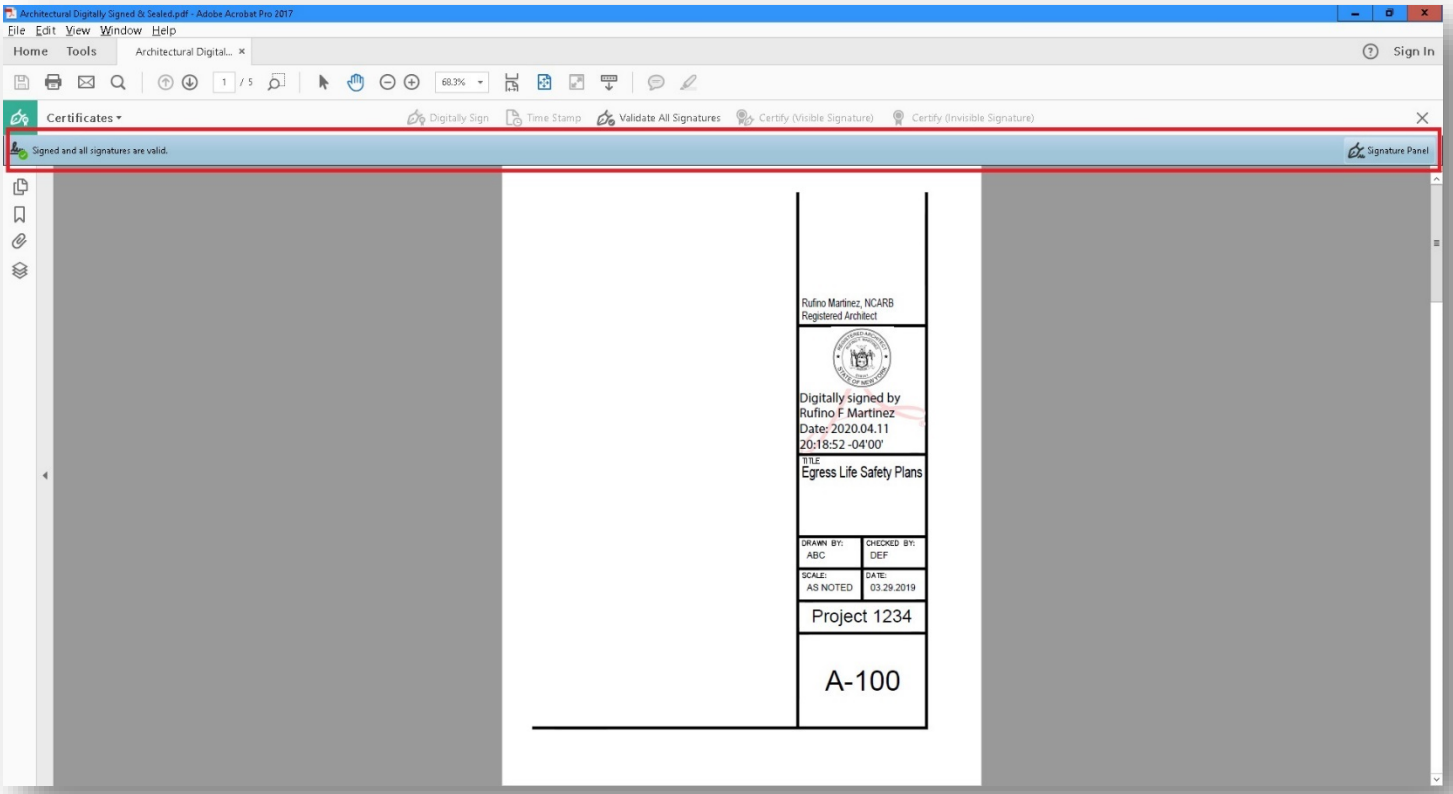
- ‘Save As PDF’ pop-up window will appear > Save over the previous file

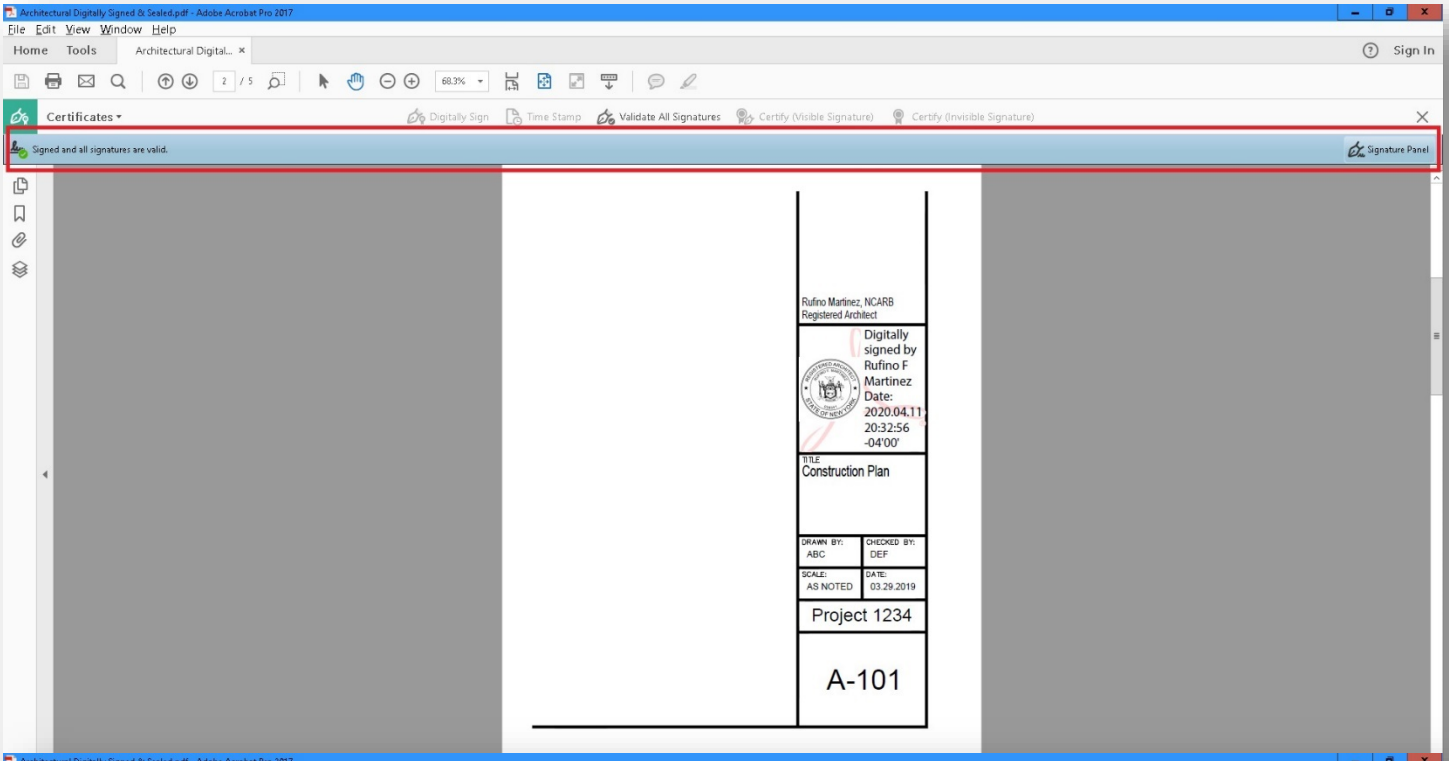


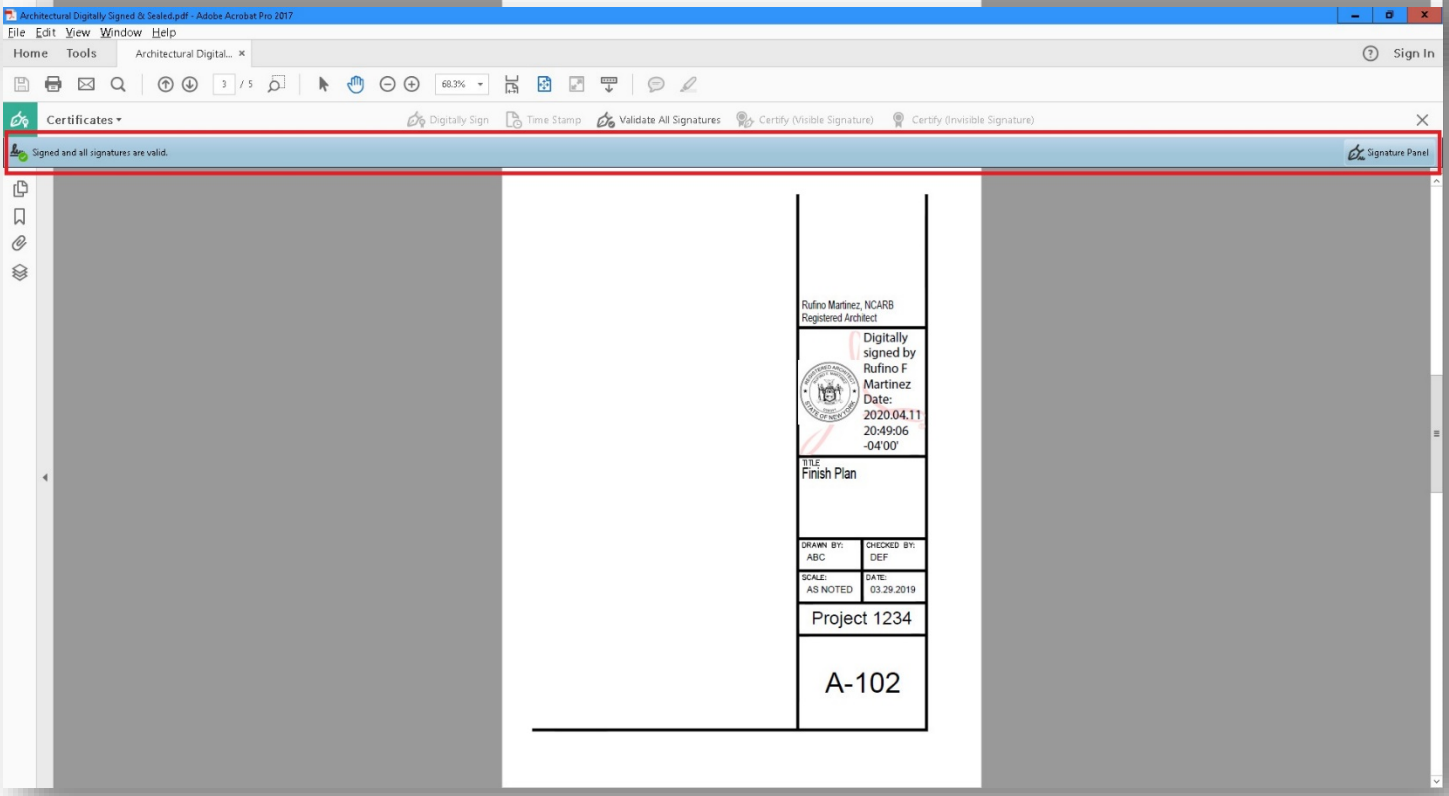
- ‘Save As’ pop-up window will appear > ‘…Replace existing file?’ > Yes

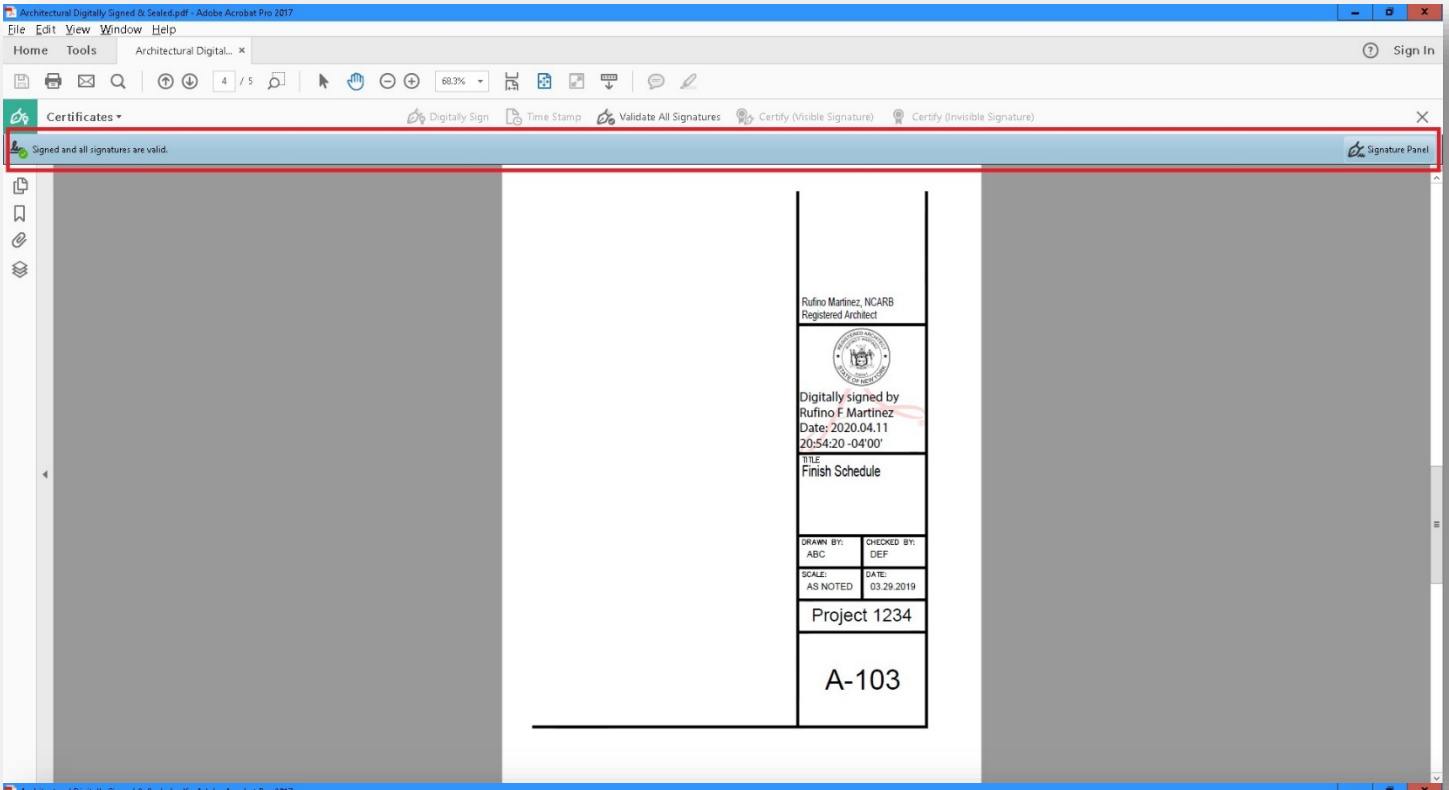


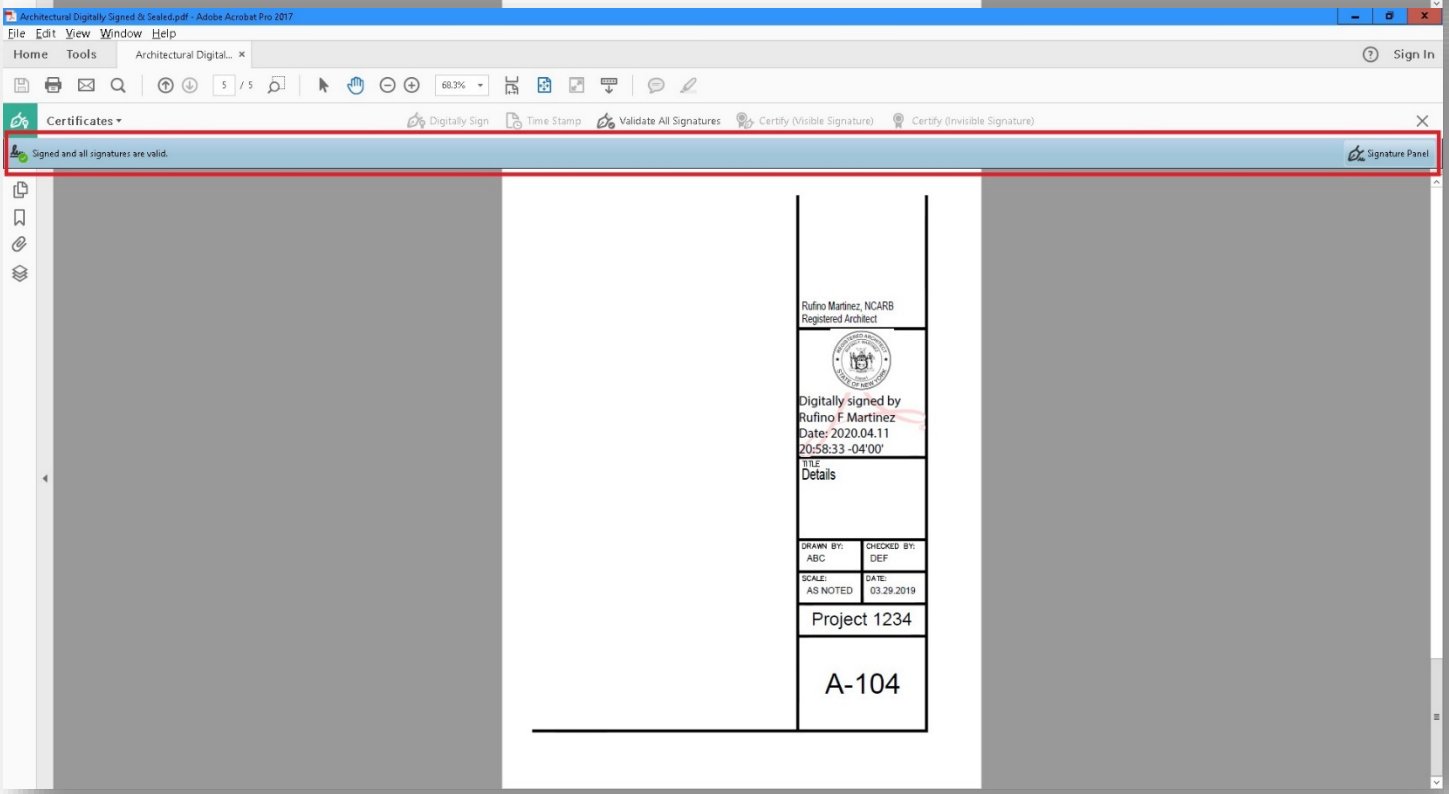
- Once the last document is digitally signed and seal and saved you will notice the blue ribbon across the top of the document to indicate all the documents of the multi-page document have been digitally signed. You will also notice that since the document was locked you no longer have the ability to digitally sign the document.




Architectural Digitally Signed & Sealed.pdf - Adobe Acrobat Pro 2017
File Edit View Window Help
Home Tools
Sign In
Certificates
Digitally Sign
Time Stamp
Validate All Signatures
Certify (Visible Signature)
Certify (Invisible Signature)
Signed and all signatures are valid.
Signature Panel
Rufino Martinez, NCARB
Registered Architect
Digitally signed by Rufino F Martinez
Date: 2020.04.11 20:32:56 -04'00'
TITLE
Construction Plan
DRAWN BY: ABC
CHECKED BY: DEF
SCALE: AS NOTED
DATE: 03.29.2019
Project 1234
A-101


Architectural Digitally Signed & Sealed.pdf - Adobe Acrobat Pro 2017
File Edit View Window Help
Home Tools
Sign In
Certificates
Digitally Sign
Time Stamp
Validate All Signatures
Certify (Visible Signature)
Certify (Invisible Signature)
Signed and all signatures are valid.
Signature Panel
Rufino Martinez, NCARB
Registered Architect
Digitally signed by Rufino F Martinez
Date: 2020.04.11 20:49:06 -04'00'
TITLE
Finish Plan
DRAWN BY: ABC
CHECKED BY: DEF
SCALE: AS NOTED
DATE: 03.29.2019
Project 1234
A-102


Architectural Digitally Signed & Sealed.pdf - Adobe Acrobat Pro 2017
File Edit View Window Help
Home Tools
Architectural Digital...
Sign In
Certificates
Digitally Sign
Time Stamp
Validate All Signatures
Certify (Visible Signature)
Certify (Invisible Signature)
Signed and all signatures are valid.
Signature Panel
Rufino Martinez, NCARB
Registered Architect
Digitally signed by
Rufino F Martinez
Date: 2020.04.11
20:54:20 -04'00'
TITLE:
Finish Schedule
DRAWN BY:
ABC
CHECKED BY:
DEF
SCALE:
AS NOTED
DATE:
03.29.2019
Project 1234
A-103

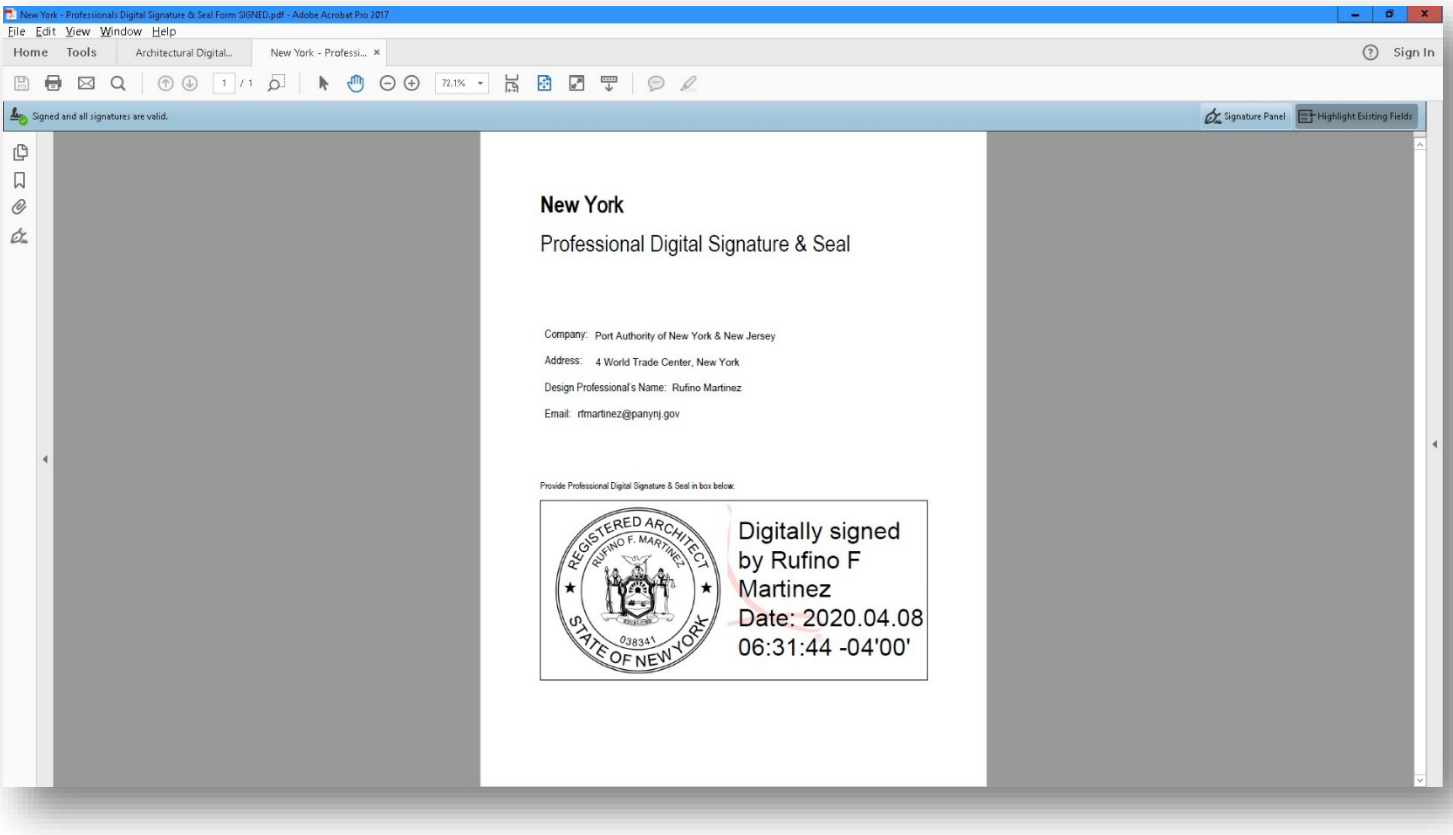

Architectural Digitally Signed & Sealed.pdf - Adobe Acrobat Pro 2017
File Edit View Window Help
Home Tools
Architectural Digital...
Sign In
Certificates
Digitally Sign
Time Stamp
Validate All Signatures
Certify (Visible Signature)
Certify (Invisible Signature)
Signed and all signatures are valid.
Signature Panel
Rufino Martinez, NCARB
Registered Architect
Digitally signed by
Rufino F Martinez
Date: 2020.04.11
20:58:33 -04'00'
TITLE:
Details
DRAWN BY:
ABC
CHECKED BY:
DEF
SCALE:
AS NOTED
DATE:
03.29.2019
Project 1234
A-104

2.11 Design Professionals – Digitally Signing & Sealing Documents

ALL Design professionals that are taking responsibility for the work submitted through the Tenant Alteration Application (TAA) process will need to digitally sign and seal their documents. This includes but is not limited to the following: Architect/Engineer of Record and all consultants (Structural, Mechanical, Electrical, Plumbing, Fire Alarm, Fire Protection, etc.) associated with the scope of work.

2.12 Professional Digital Signature & Seal Form

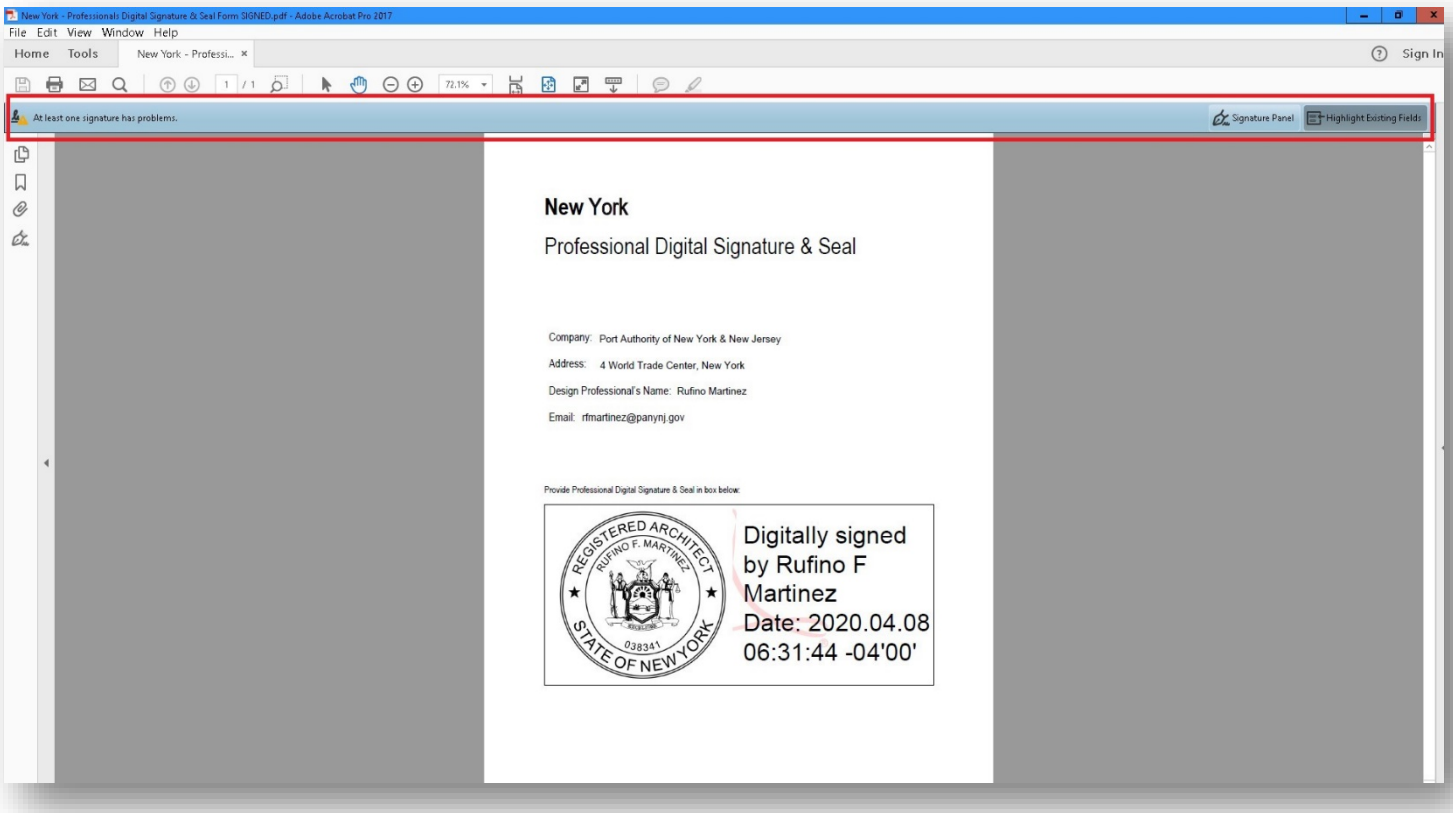
All design professionals that will be digitally signing and sealing documents shall complete the Professional Digital Signature & Seal Form. Once completed, this form shall be used by the Port Authority Quality Assurance Division – Design Standards Unit to confirm that the digital signature and seal is in compliance with the criteria outlined in The Port Authority Digital Signature & Seal Policy.



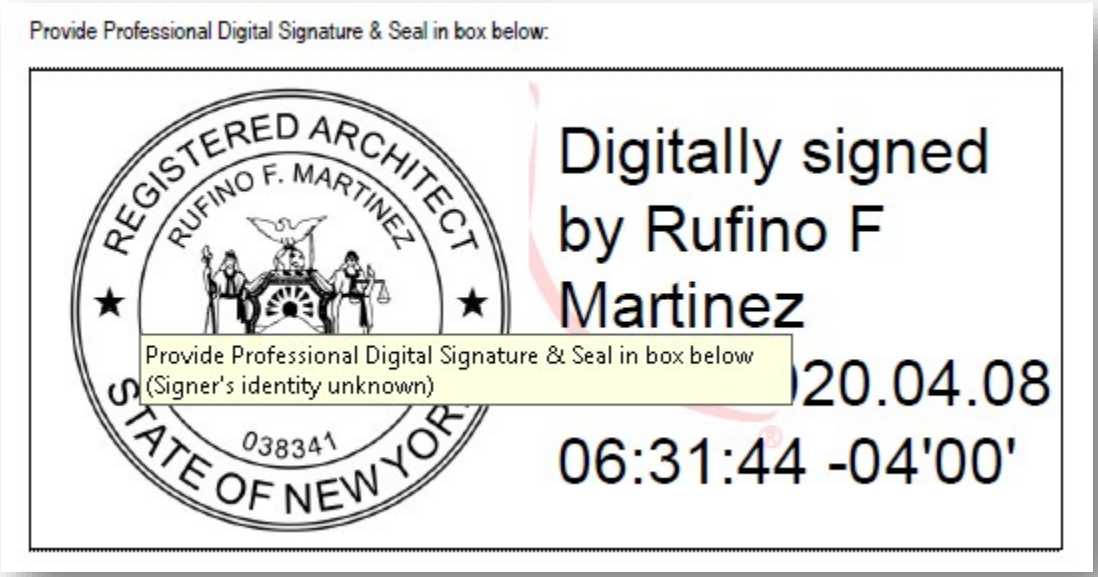
2.13 How the Port Authority of New York & New Jersey Verifies the 'Digital Certificate'

Once the Quality Assurance Department – Design Standards Unit receives the Professional Digital Signature & Seal Form we review the digital certificate to confirm that the digital signature and seal is in compliance with the criteria outlined in The Port Authority Digital Signature & Seal Policy.

- Opening the document, we can determine by the blue ribbon across the top of the document that indicates the document has been digitally signed.

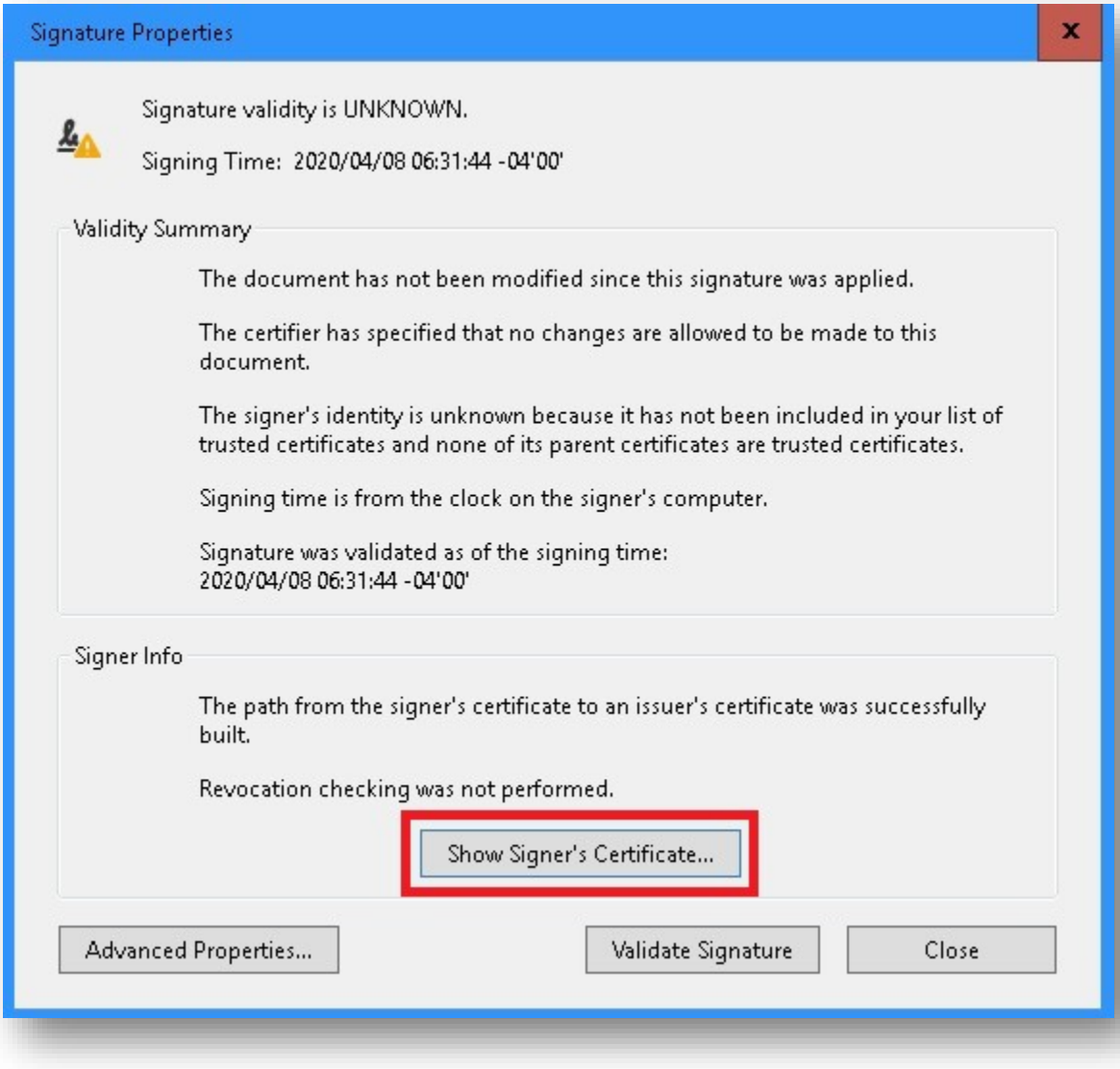


- Double clicking on the digital signature & seal will bring us to the 'Signature Validation Status'



- The 'Signature Validation Status' pop-up window will appear > 'Signature Properties…'

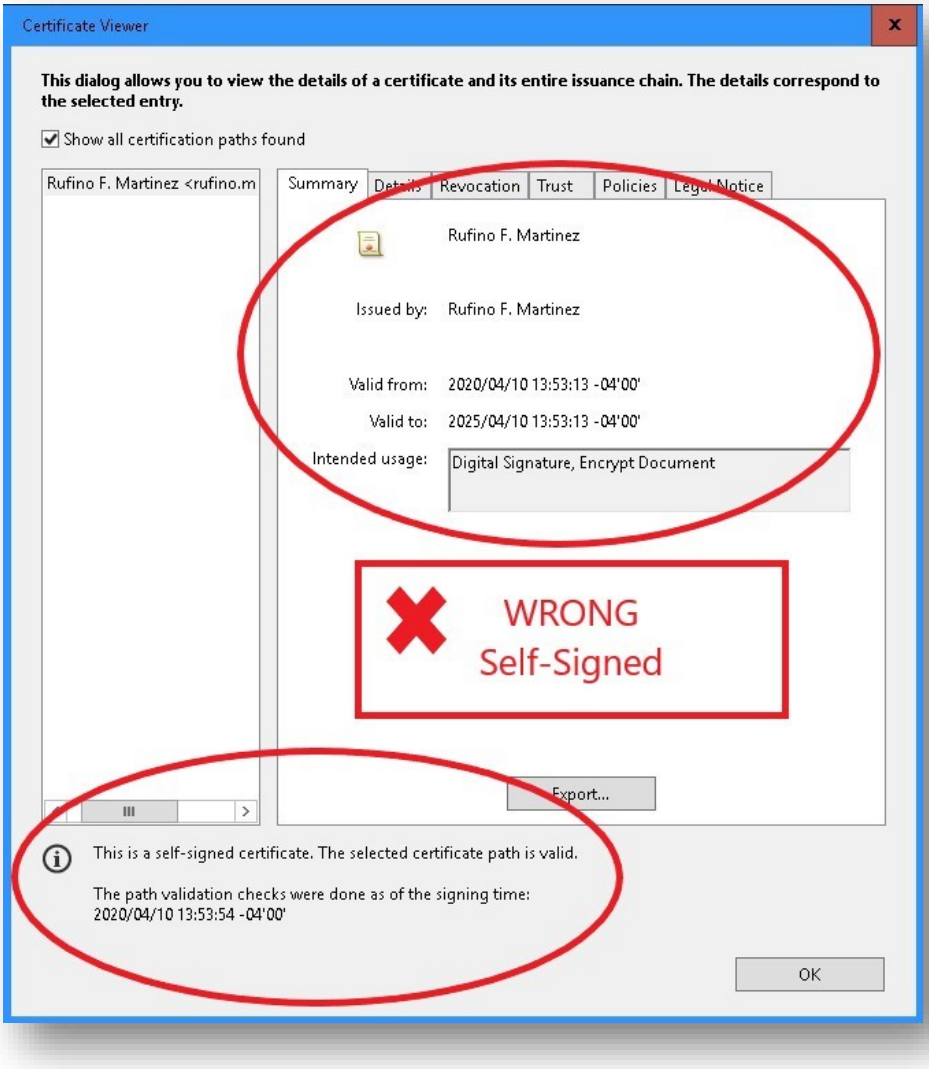
o The 'Signature Properties' pop-up window will appear > 'Show Signer's Certificate…



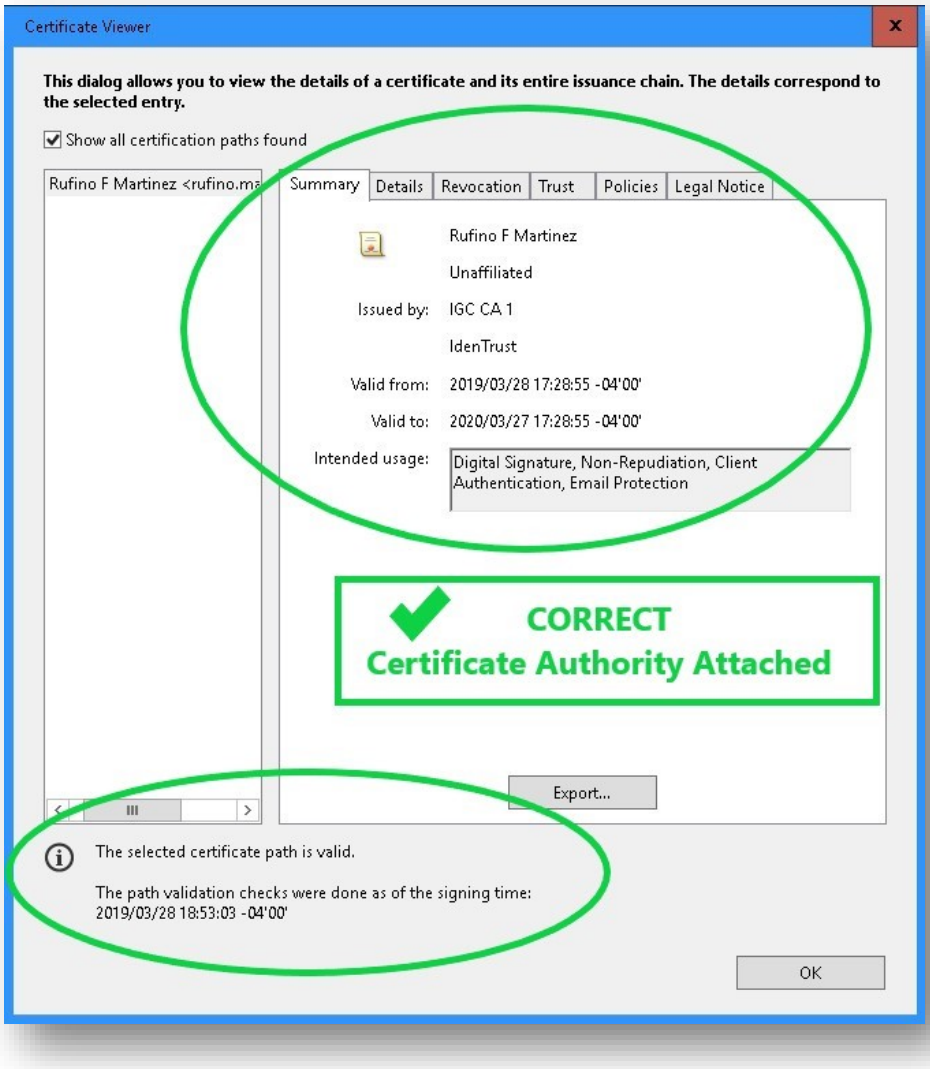
o The 'Certificate Viewer' pop-up window will appear.

IMPORTANT
YOU CANNOT SELF-SIGN YOUR DIGITAL SIGNATURE. Design Professionals signatures and seals shall meet the requirements of Digital Signature Standard (DSS) established by the National Institute of Standards and Technology and published by the United States Department of Commerce in publication, Federal Information Processing Standards Publication (FIPS PUB) 186-4 (2013). The digital signature must be verifiable by a trusted third party. A digital signature algorithm allows an entity to authenticate the integrity of signed data and the identity of the signatory. The recipient of a signed message can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory.

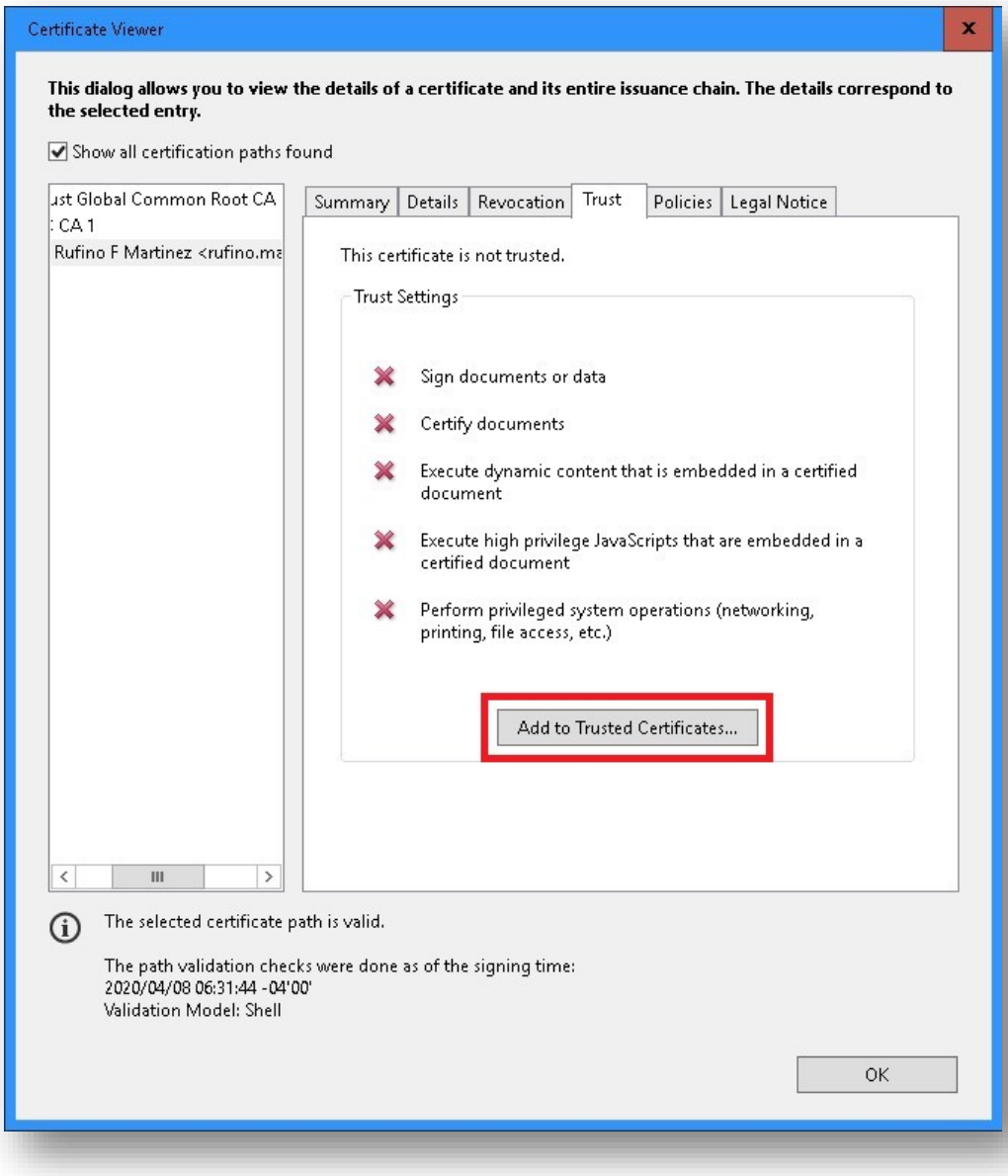
o The 'Certificate Viewer' pop-up window below indicates a 'Self-Signed Certificate'
THIS IS NOT A VALID DIGITAL SIGNATURE.



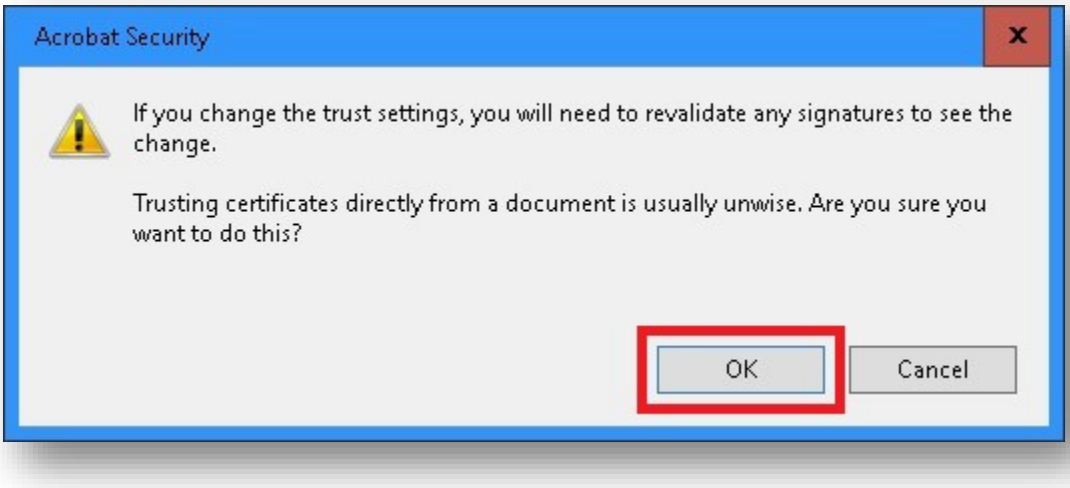
o The ‘Certificate Viewer’ pop-up window below indicates a ‘Certificate Authority’ is issued by a verifiable trusted Third Party.



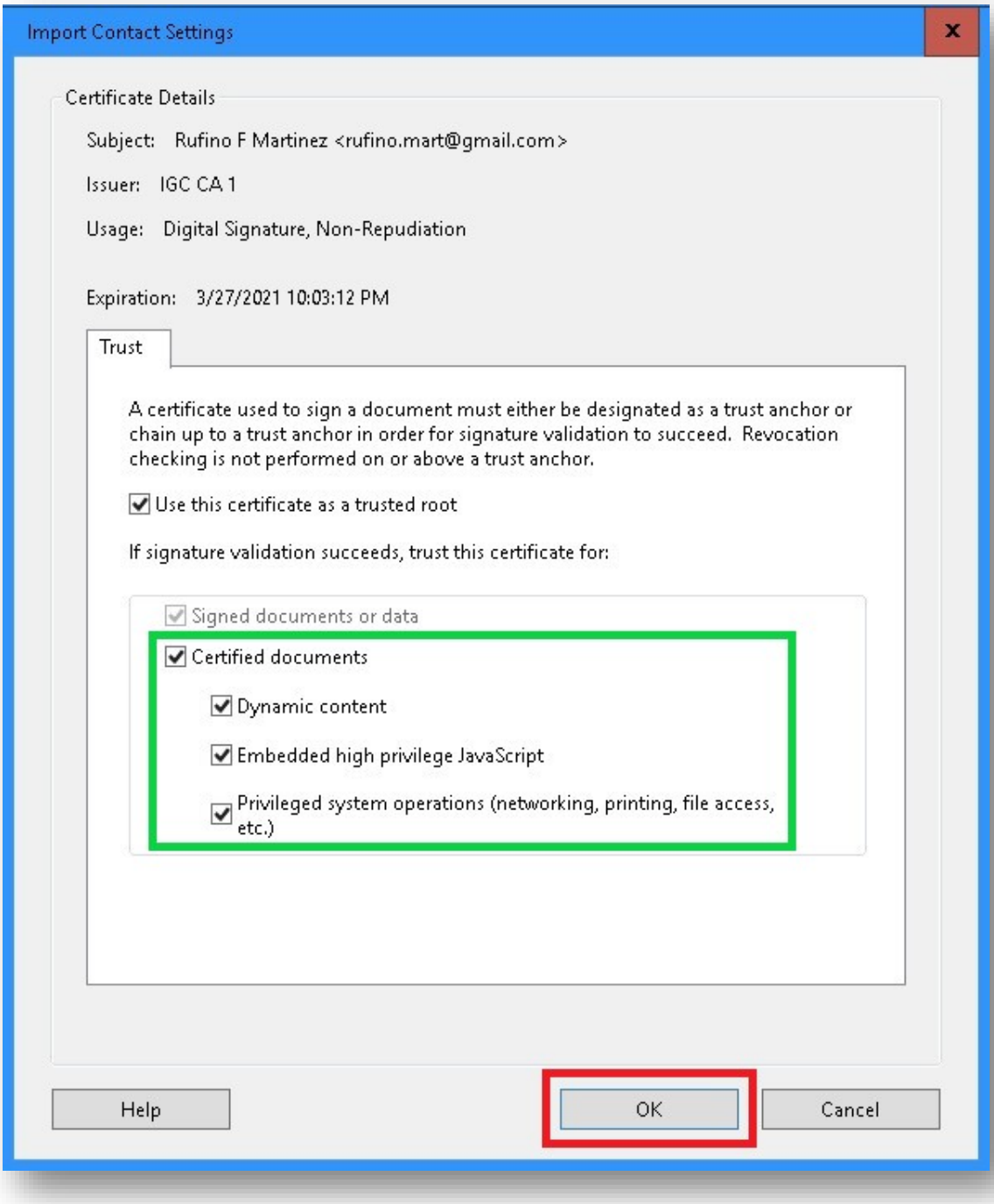
o Select the 'Trust' tab on the 'Certificate Viewer' pop-up window > Select 'Add to Trusted Certificates…'



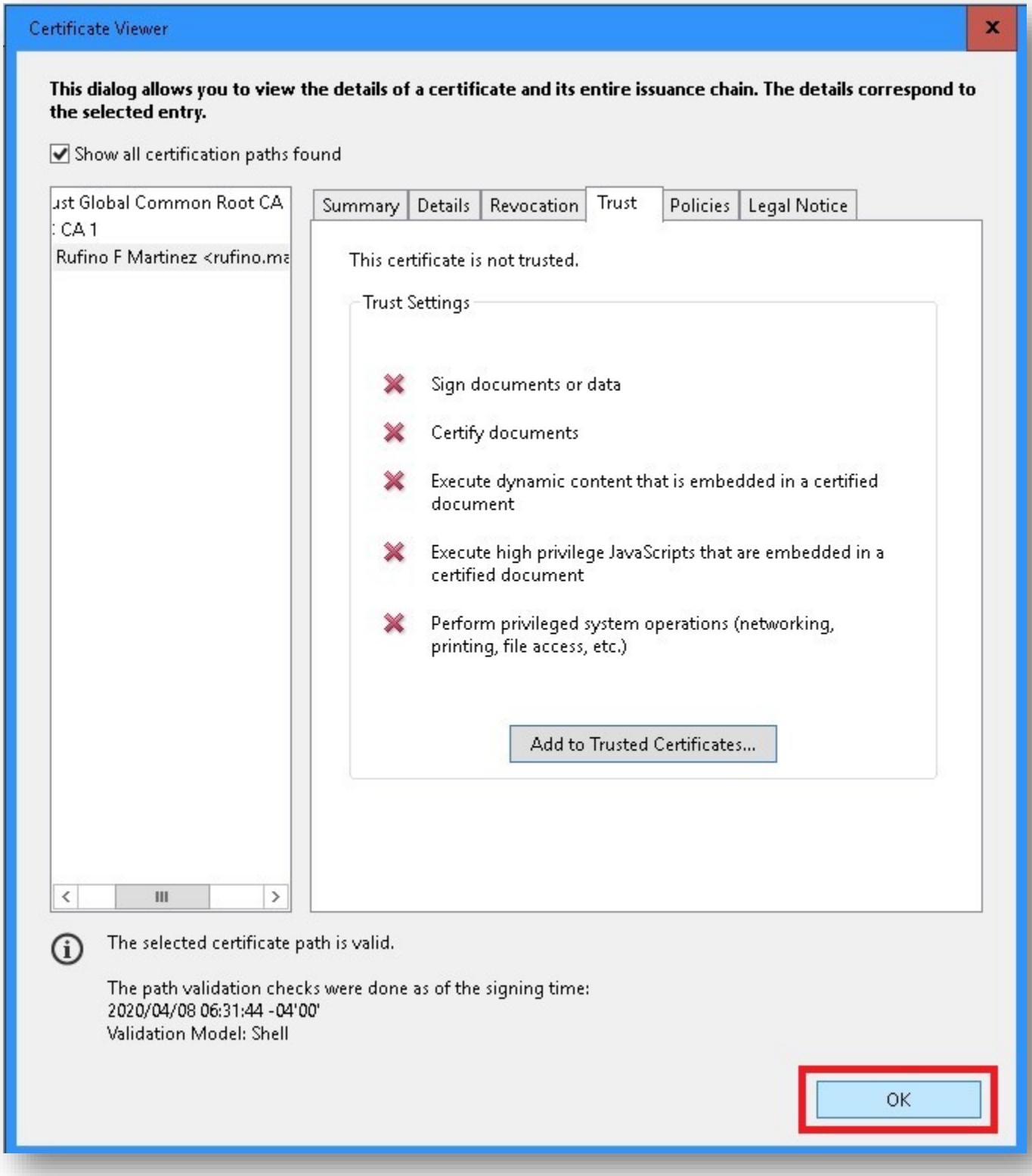
o The ‘Acrobat Security’ pop-up window will appear > ‘OK’



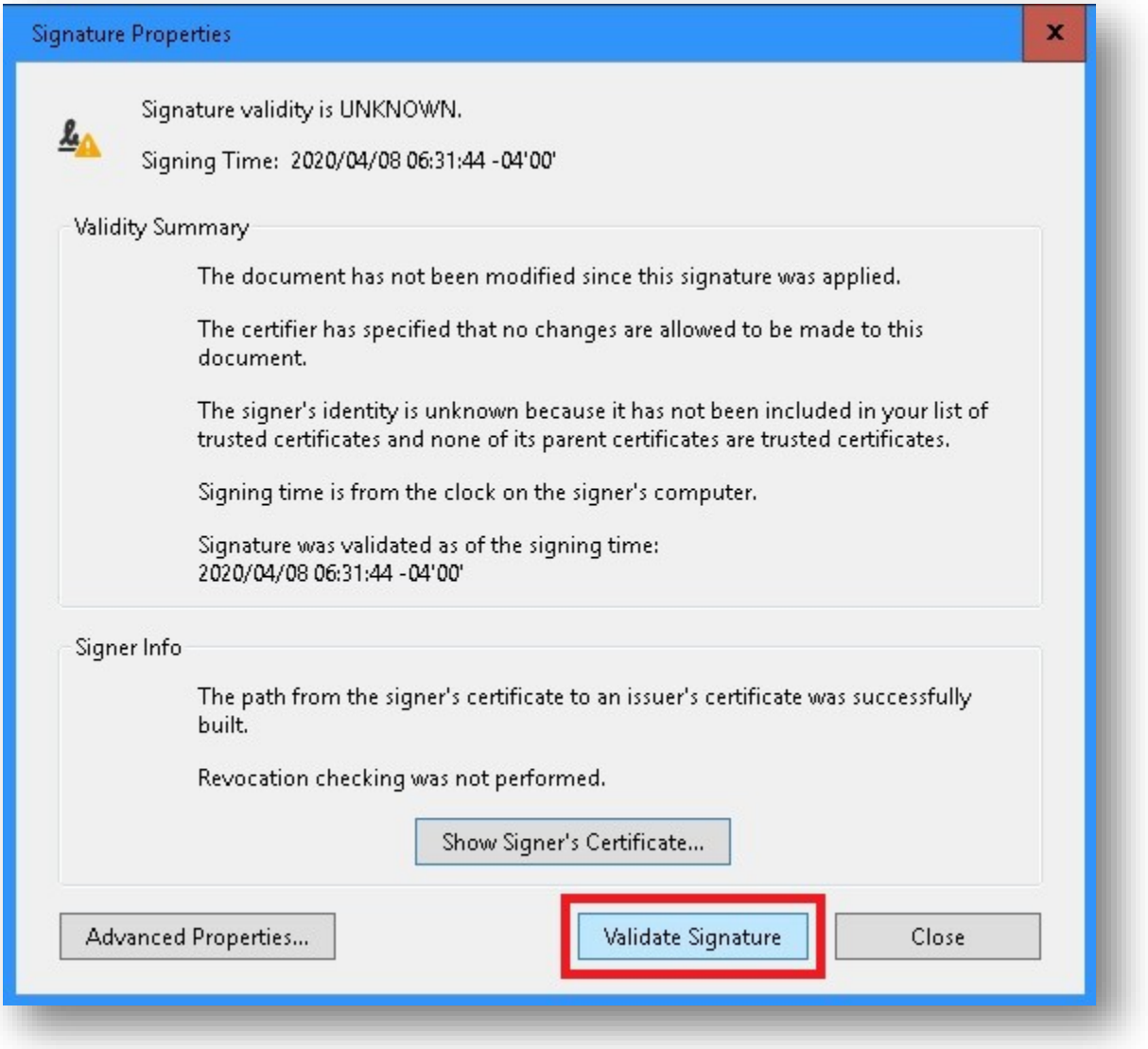
o The 'Import Contact Settings' pop-up window will appear > Select 'Certified documents' > 'Dynamic content' > 'Embedded high privilege JavaScript' > 'Privileged system operations' > 'OK'



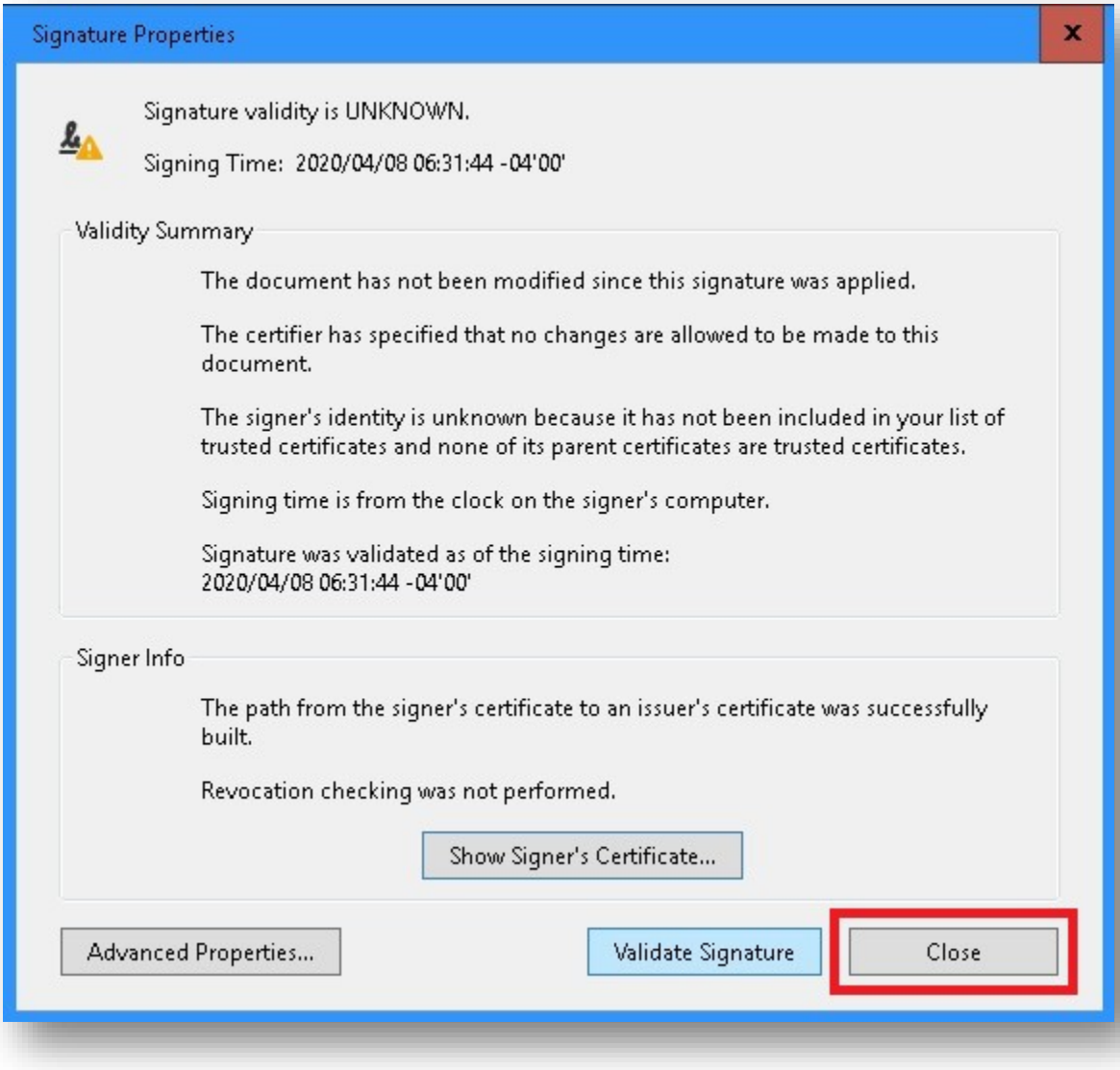
- The 'Certificate Viewer' pop-up window will appear > 'OK'



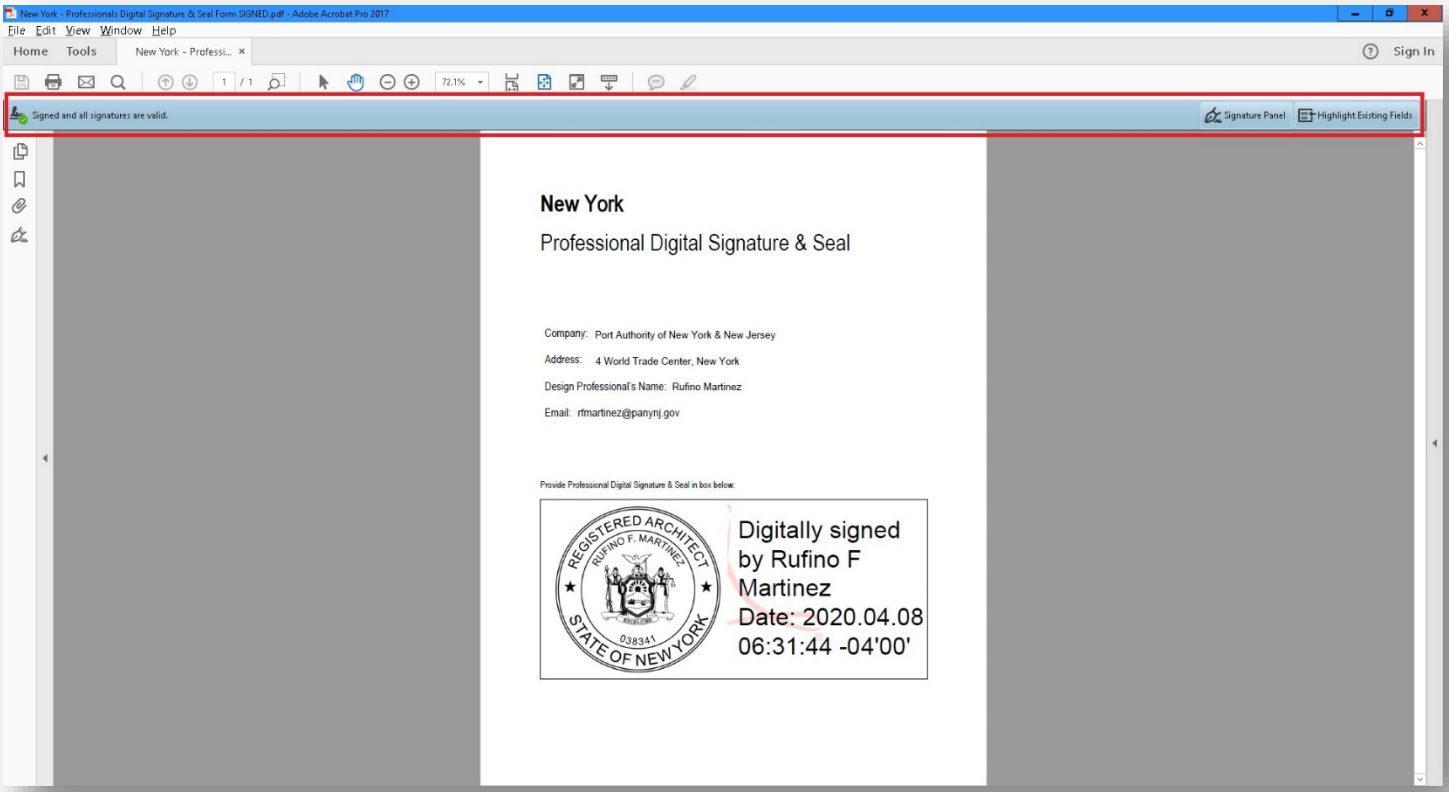
- The 'Signature Properties' pop-up window will appear > 'Validate Signature'



o Select 'Close'. Once refreshed, the document will display a blue ribbon across the top of the document that indicates the validated status of the signature.

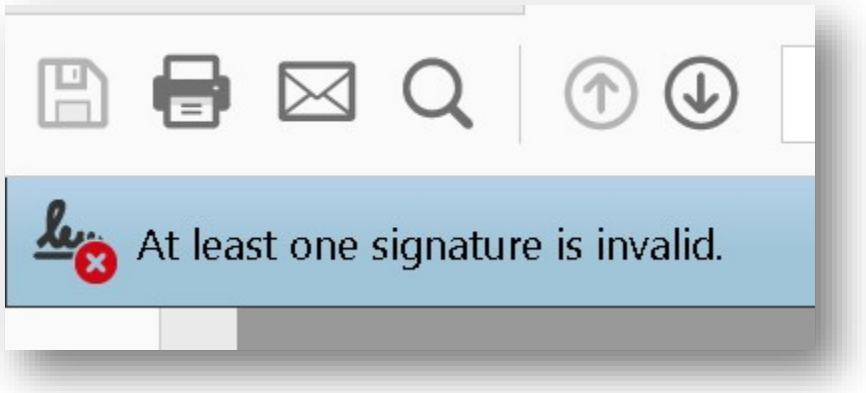


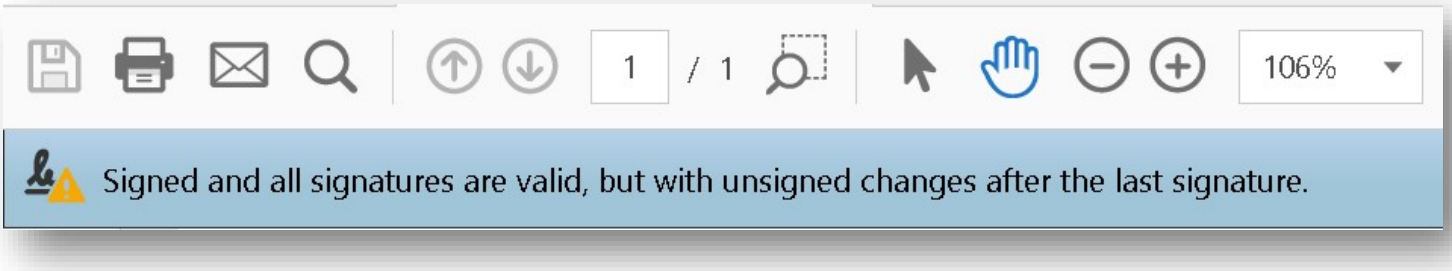
- Opening the document, we can see a green check mark on the blue ribbon across the top of the document, this indicates that the document has been digitally signed and successfully verified.



2.14 Resolving Errors Prior to Submission

It is the responsibility of the design professional to ensure that their digital signature and seal are submitted without error. All errors must be resolved prior to submittal. Submissions that display *'At least one signature is invalid'* on the blue ribbon across the top of the document, will **NOT** be accepted. This means the Document has been altered or corrupted since it was signed. This can happen if someone alters the document after it was digitally signed, or it could be that someone else tried to digitally sign the document after it was already digitally signed by someone else.



2.15 Changes After Digitally Signed and Sealed

It is the responsibility of the design professional to ensure that there are no changes to the PDF document once it is digitally signed and sealed. **Changes that are made after it is digitally signed and sealed will invalidate the signature.** Submissions that display *'Signed and all signatures are valid, but with unsigned changes after the last signature'* on the blue ribbon across the top of the document, will **NOT** be accepted.