

NOTICE

The audio portion of this on-demand webinar was recorded at the 2017 Professional Engineers Conference. The audio and the powerpoint presentation were combine to make the on-demand webinar. The on-demand webinar experience will differ from those attending the conference interacting with the instructor .

NOTICE

The NSPE live webinar is presented and copyrighted by the National Society of Professional Engineers®. All rights are reserved. Any transmission, retransmission or republishing of the audio or written portions of this program without permission of the National Society of Professional Engineers® is prohibited.

20 Professional
17 Engineers
CONFERENCE



Going Digital: Digital Signatures & Digital Document Delivery

Peter McConaughy, PE

NSPETM NATIONAL SOCIETY OF
PROFESSIONAL ENGINEERS

Learning Objectives

- Review current legalities regarding digital signatures
- Discuss the pros and cons of available digital signature options
- Identify best practices for new digital technology

Introduction

Founder of McCon Engineering, Inc. (4/1/2000-Present)

I am a licensed Structural Engineer (MD, VA, PA, DE)

Co-Founder of Seal Authority LLC (8/11/2015-Present)

An online document delivery portal for design professionals

Disclaimers

I am not an attorney; this is not legal advice.

I am not a computer geek; this is not a technical study of Digital Signatures

I am not promoting any particular product . . .

but I will be happy to answer questions if I can

Peter McConaughy, PE

410-652-3635

Peter@SealAuthority.com

www.SealAuthority.com



SealAuthority
ENHANCED DOCUMENT SECURITY

Slide 5 of 31

Definitions

Signature

That mechanism by which a designer takes upon himself the professional responsibility for the content of a document.

E-Signature

Electronic signature of any kind

A mark, sound, sequence or action applied electronically with intent to sign or give consent

Digital Signature

1. A special type of E-Signature that uses PKI Asymmetric Encryption to assure that the file is not modified after signing. (Tamper proofing)
2. A secure electronic signature that passes the three question test for document integrity.

Definitions

.PDF

Portable Document Format

patent held by Adobe till 2008

was at one time difficult to modify

PKI

Public Key Infrastructure

CA

Certificate Authority –

Assigns & Registers Key Pair Certificates

AATL

Adobe Approved Trust List

List of 58+ CA's recognized by Adobe Reader

Asymmetric Encryption a form of encryption based on a Key Pair in which the Private Key encrypts a message that only the Public Key can decrypt.

E-Sign Act of 2000

E-Sign Act

- Electronic Signatures In Global & National Commerce Act
- Enacted by Federal Government to promote E-Commerce
- All parties must agree on:
 - Use of digital signatures
 - Choice of software used for verification
 - Notify each other if software changes
 - Either party can request a paper copy anytime
 - Location of original document
- Limited to contractual agreements



E-Sign Act of 2000

Effect of E-Sign Act

E-Signature legally equal to Wet Signature

- Some exceptions apply for highly regulated industries

E-signature not sufficient

- Digital Signatures Required
- Must be authenticated by third party



E-Sign Act of 2000

Engineers issue documents

“To Whom It May Concern”

- Drawings are relied upon by the public at large
- Interested parties are not usually party to a contract

In this context, the E-Sign Act does not apply, as its requirements cannot be satisfied

- Never agreed to use of digital signatures
- May not have the software or knowledge
- Do not have option to request paper copy
- Cannot be notified of software changes

(This is not like buying a house)



Digital Signatures for Engineers

NCEES Model Law

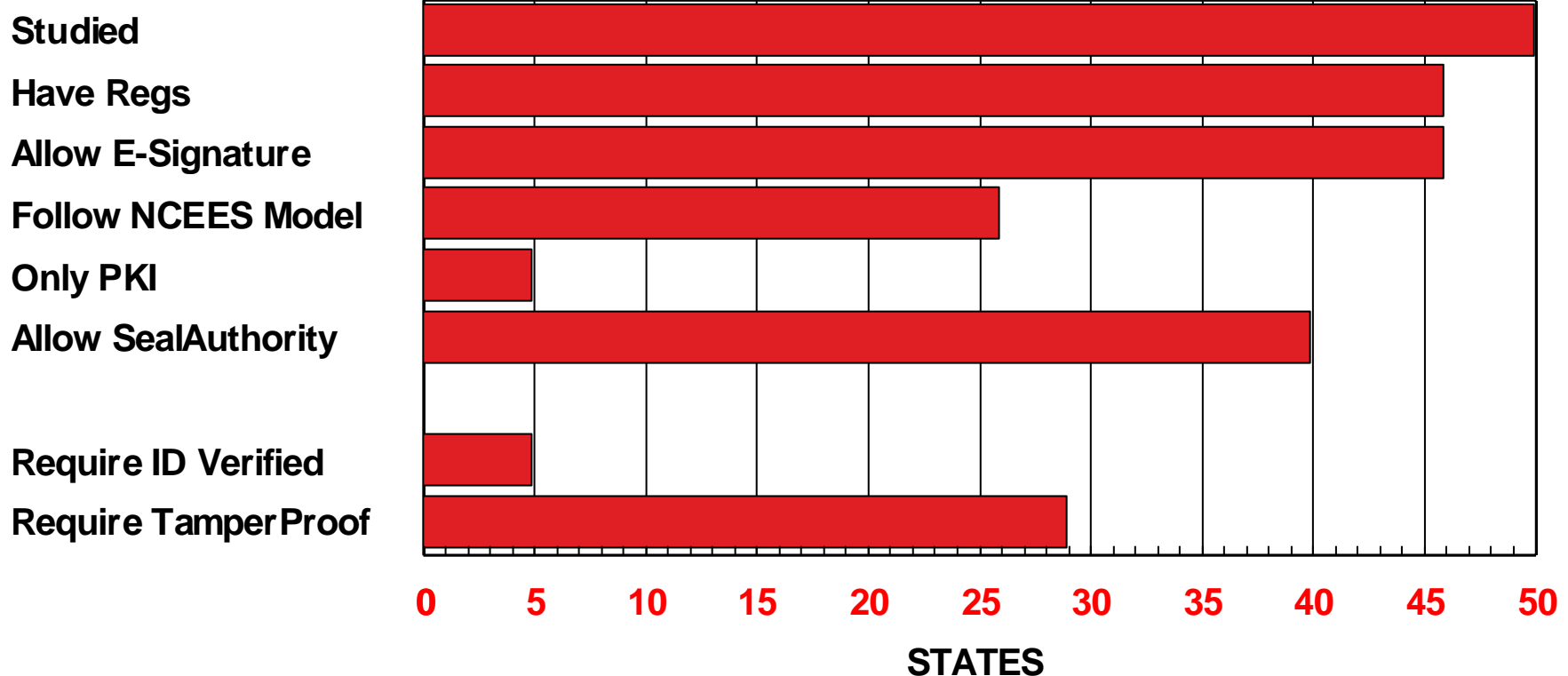
Drawings, reports, and documents that are signed using a digital signature **must** have an electronic authentication process attached to **or** logically associated with the electronic document.

The digital signature must be

1. Unique to the individual using it
2. Capable of verification
3. Under the sole control of the individual using it
4. Linked to a document in such a manner that the digital signature is invalidated if any data in the document is changed

Digital Signatures for Engineers

State Regulations On Digital Signatures for Engineers



Digital Signatures for Engineers

By signing a document, you accept professional responsibility for its content.



Your digital signature must do two things:



1. Prevent impostors from signing in your name, and



2. Prevent modification of the document after signing

Slide 13 of 31

Digital Signatures for Engineers

3 Question Test for Document Integrity:

1. Was it Signed/Sealed?

Does the issuer take responsibility?
(capable of verification, non-repudiation)



2. Do we know the source?

Or is it a forgery?
(identification, exclusive control)



3. Is this the document?

Or was it modified after signing?
(invalidation)



Signature Options

- 1. Wet Signature**
- 2. E-Signature**
- 3. PKI Digital Signature (Self-Signed)**
- 4. PKI Digital Signature (Third Party Verified)**
- 5. SealAuthority (Direct Document Delivery)**

Signature Options

1. Wet Signature

- Familiar
- Not without risks
- Defines the minimum acceptable security for digital signatures

Dear Client,

The signature below was made by my own hand. You can try to copy it if you like, but handwriting experts can likely identify the forgery.

You can also try to copy my seal, but since it was applied with wet ink, that will be rather difficult – unless of course you purchase a copy of my stamp for yourself, in which case you might succeed (for a while) at issuing documents in my name.

Was it signed/sealed?	yes
Do we know the source?	yes
Is this the document?	yes



Sincerely,

Peter McConaughy, PE
Co-Founder

Signature Options

2. E-Signature

- PIN #
- Click-thru software
- Check mark
- Password, key phrase, secret question
- Initials, Full name
- Graphic block

Was it signed/sealed? ??
 Do we know who signed? ??
 Is this the document? ??

Dear Client,

The signature below demonstrates my trust in your fine moral character.

I know that you could edit the body of this Word, AutoCad or .PDF document however you like, and then forward it to others over my signature. Or you could paste my seal into your own document just as easily as I pasted it here. And since my signature is just text on the page, you can also sign my name to whatever you wish simply by using the same font.

I'm sure you will not do those things.



Sincerely,

Peter McConaughy

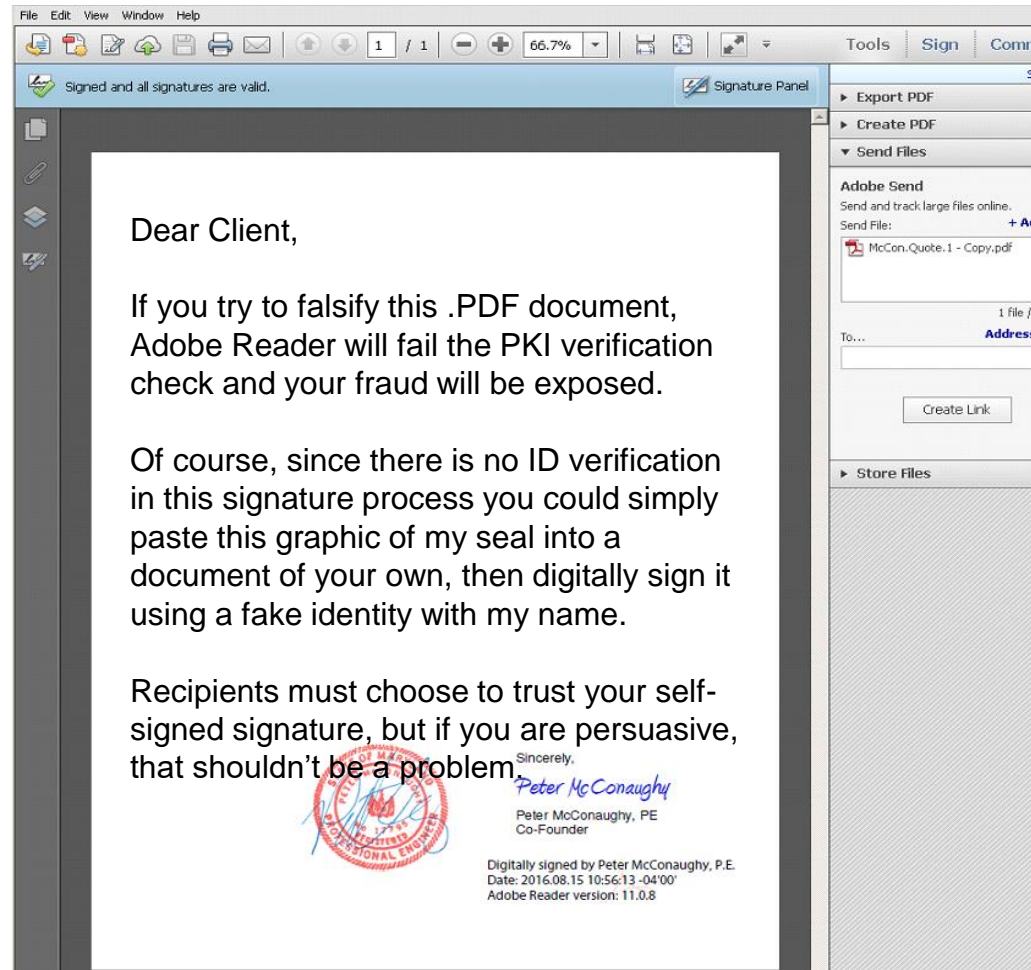
Peter McConaughy, PE
 Co-Founder

Signature Options

3. PKI Digital Signature (Self-signed)

- Available through Adobe Reader
- Tamper proofs the document
- Your Certificate must reside on the recipient's computer
- Signature is not visible on document
- Cannot be inspected once printed
- Easy to create, easy to falsify

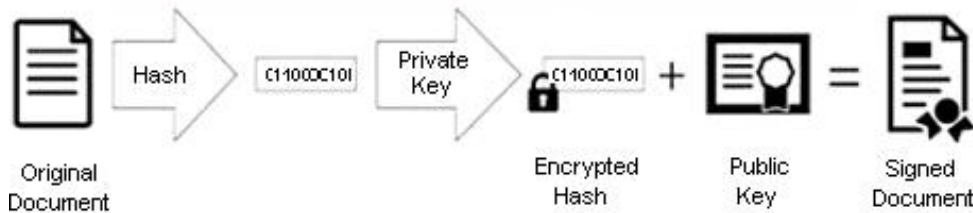
Was it signed/sealed? **yes**
 Do we know the source? **??**
 Is this the document? **yes**



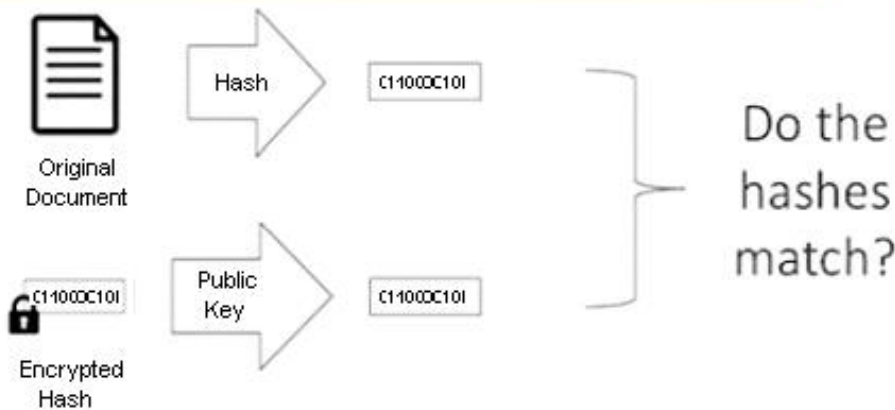
Signature Options

How PKI Signatures Work (As explained by GLOBALSIGN)

APPLYING THE SIGNATURE



VALIDATING THE SIGNATURE



ARE WE GETTING **WHAT WE NEED** FROM DIGITAL SIGNATURES?

- ✓ Integrity – hash check
- ✓ Authenticity – public key
- ✓ Non-repudiation – asymmetric encryption

Yes **As Long As:**

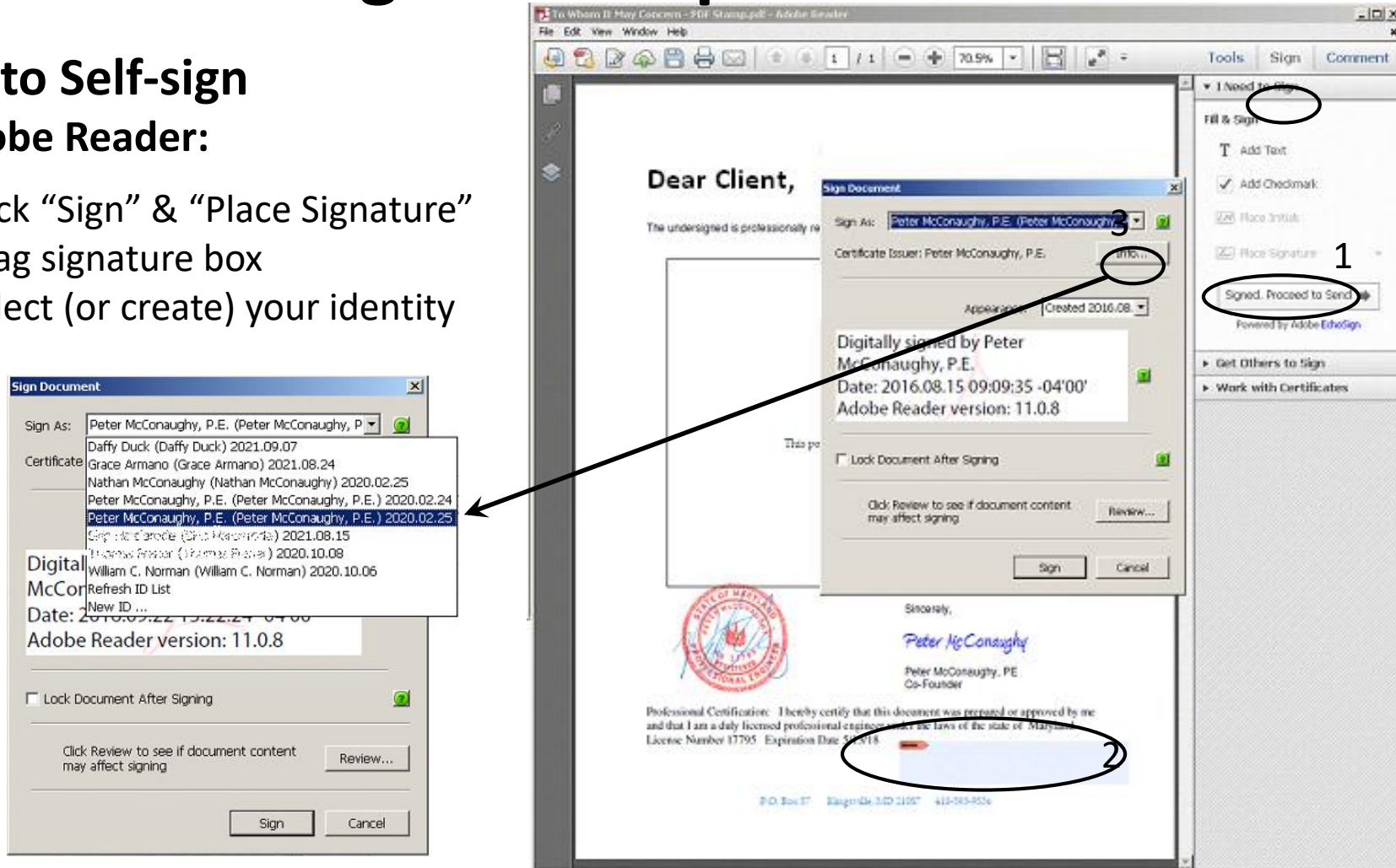
- The certificate is valid & current
- The private key is not compromised
- The recipient is wise & diligent
- You have the required software
- The software works as intended
- The document is never printed
- Certificate holder's ID is verified

Slide 19 of 31

Signature Options

How to Self-sign In Adobe Reader:

1. Click “Sign” & “Place Signature”
2. Drag signature box
3. Select (or create) your identity



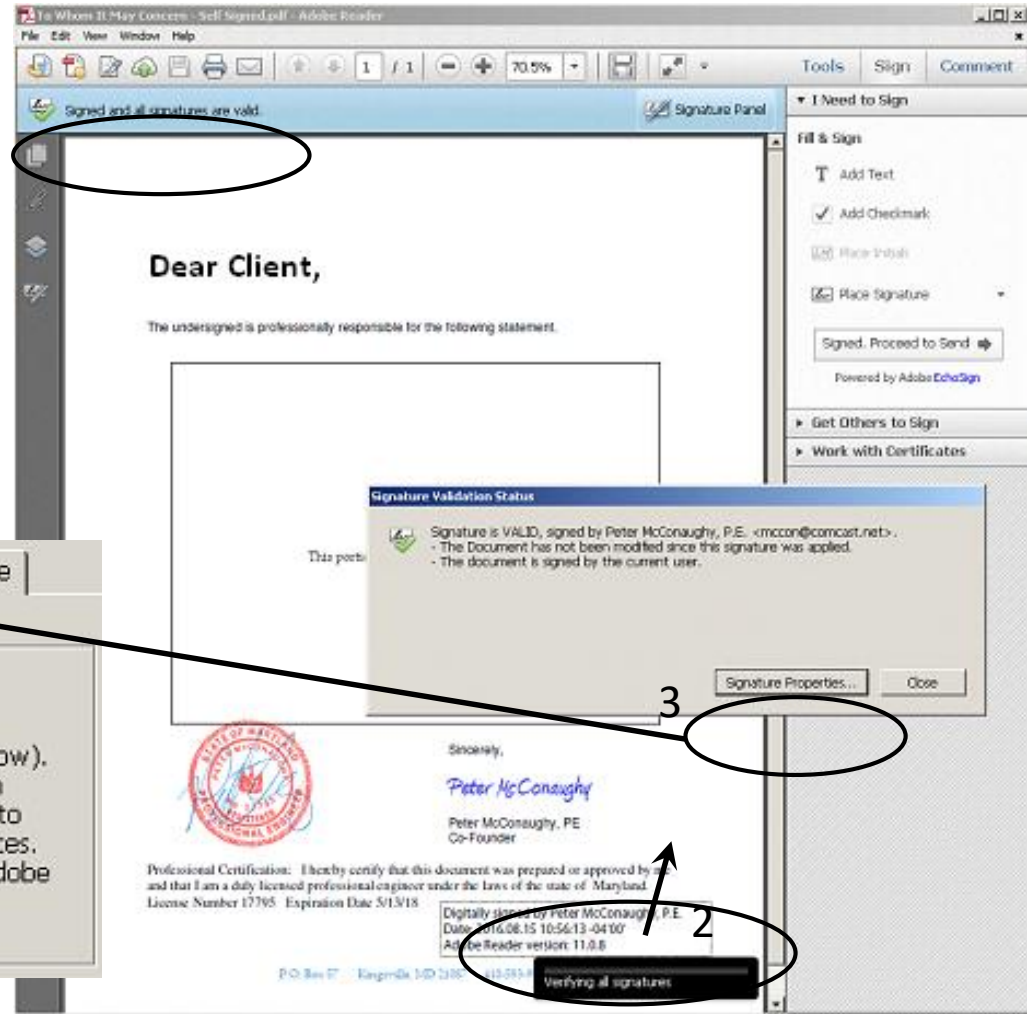
“You can be whoever you want to be.”

Signature Options

How to Verify a Signature

1. Adobe Reader shows status
2. Must click the signature
3. Certificate must reside on the recipient's computer (or the web)

Multiple cautions erode the significance of a true negative



Summary | Details | Revocation | Trust | Policies | Legal Notice

Legal Disclaimer

Validation of a digitally signed document may require certificate-related services provided by independent third-party service vendors (see Issuer's User Notice below). Adobe does not provide any warranties of any kind with respect to digitally signed documents, certificates used to create digitally signed documents, and any related services. For further information, please review the Acrobat or Adobe Reader End User License Agreement and the Issuer Certificate Information and Policy Statement.

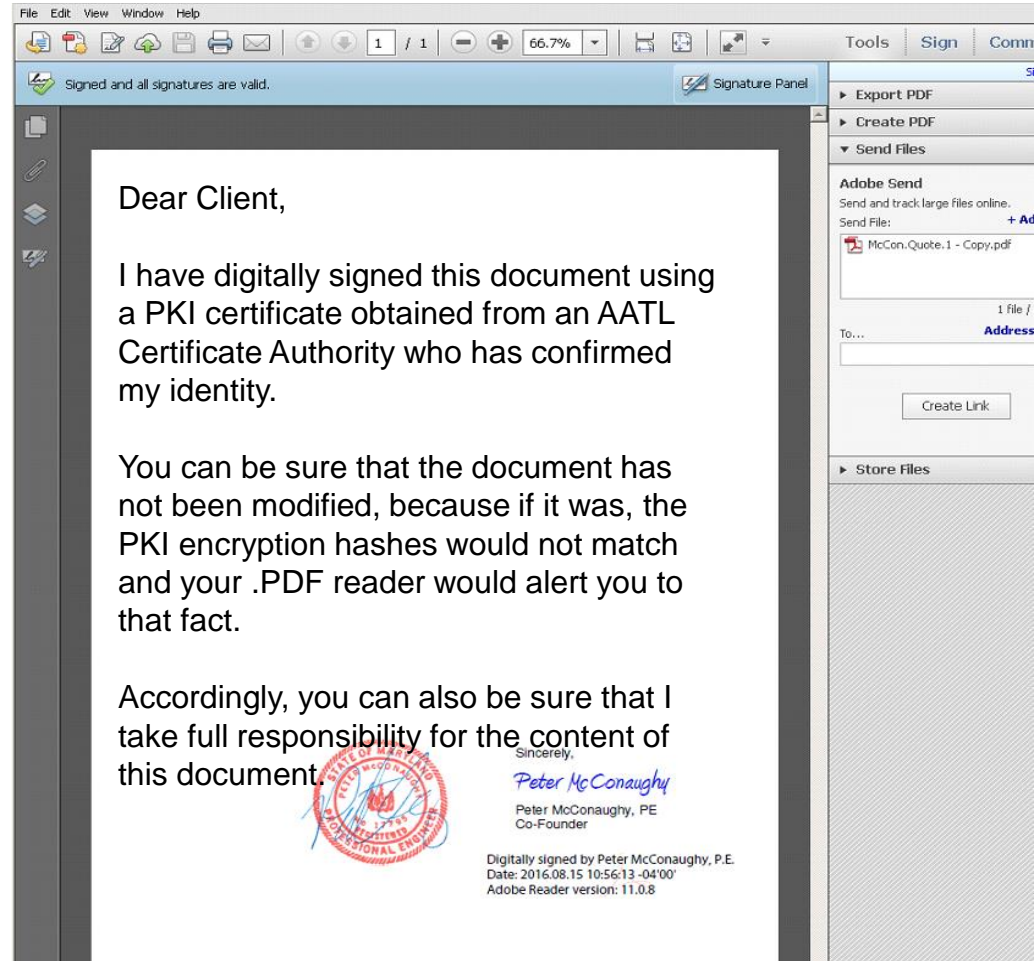
Adobe's disclaimer

Signature Options

4. PKI Digital Signature (Third Party Verified)

- Requires AATL CA to verify ID
- 2 factor ID verification via token
- Requires software to read token
- Signature is not visible
- Cannot be inspected once printed
- Once sent, we have no control

Was it signed/sealed? **yes**
 Do we know the source? **yes**
 Is this the document? **yes**



Signature Options

4. PKI Digital Signature (Third Party Verified)

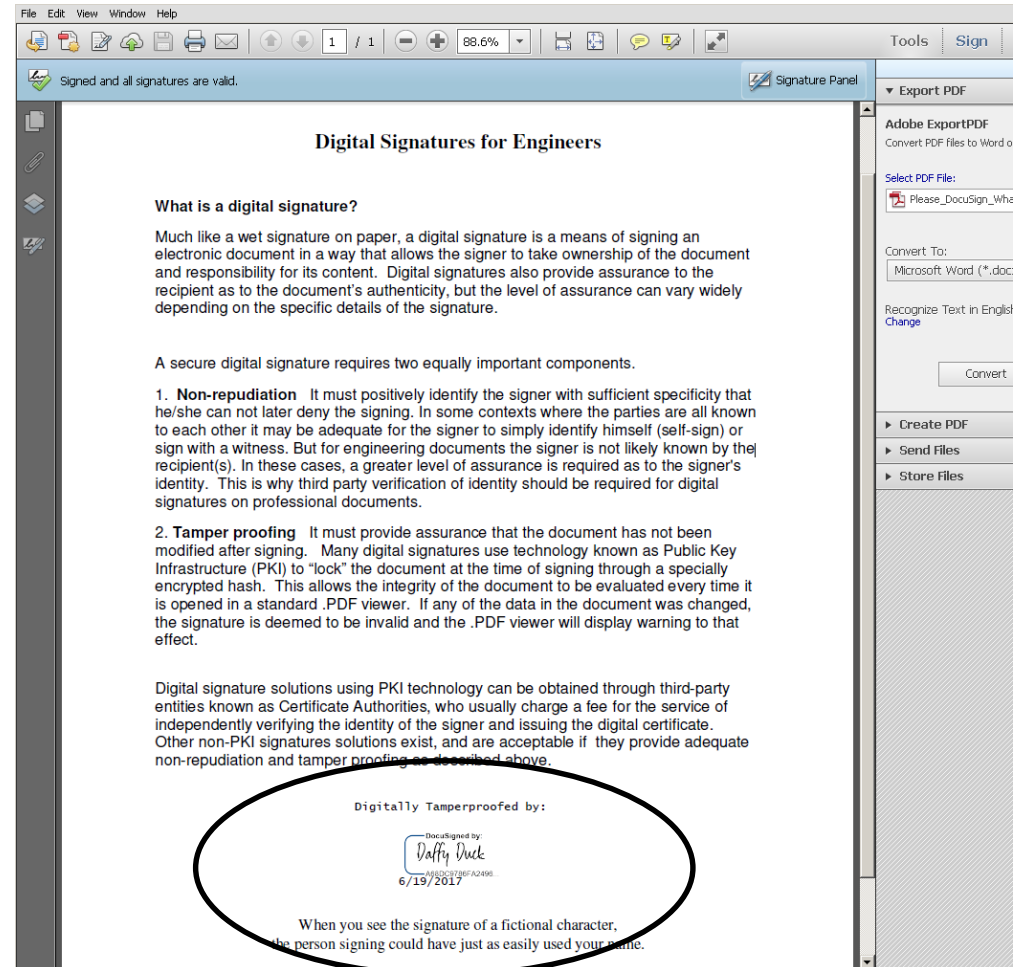
- Not All PKI Certificates are alike
- Products vary in level of Trust

Digitally Tamperproofed by:

DocuSigned by:

 A88DCB786FA2498...
 6/19/2017

When you see the signature of a fictional character, the person signing could have just as easily used your name.



The screenshot shows a PDF viewer interface. The document title is "Digital Signatures for Engineers". The content includes:

What is a digital signature?
 Much like a wet signature on paper, a digital signature is a means of signing an electronic document in a way that allows the signer to take ownership of the document and responsibility for its content. Digital signatures also provide assurance to the recipient as to the document's authenticity, but the level of assurance can vary widely depending on the specific details of the signature.

A secure digital signature requires two equally important components.

- 1. Non-repudiation** It must positively identify the signer with sufficient specificity that he/she can not later deny the signing. In some contexts where the parties are all known to each other it may be adequate for the signer to simply identify himself (self-sign) or sign with a witness. But for engineering documents the signer is not likely known by the recipient(s). In these cases, a greater level of assurance is required as to the signer's identity. This is why third party verification of identity should be required for digital signatures on professional documents.
- 2. Tamper proofing** It must provide assurance that the document has not been modified after signing. Many digital signatures use technology known as Public Key Infrastructure (PKI) to "lock" the document at the time of signing through a specially encrypted hash. This allows the integrity of the document to be evaluated every time it is opened in a standard .PDF viewer. If any of the data in the document was changed, the signature is deemed to be invalid and the .PDF viewer will display warning to that effect.

Digital signature solutions using PKI technology can be obtained through third-party entities known as Certificate Authorities, who usually charge a fee for the service of independently verifying the identity of the signer and issuing the digital certificate. Other non-PKI signatures solutions exist, and are acceptable if they provide adequate non-repudiation and tamper proofing as described above.

The signature block at the bottom of the page is circled in black and contains the text: "Digitally Tamperproofed by: DocuSigned by: Daffy Duck A88DCB786FA2498... 6/19/2017". Below the signature, the text reads: "When you see the signature of a fictional character, the person signing could have just as easily used your name."

Signature Options

5. SealAuthority (Direct Document Delivery)

- Third-Party ID verification
 - Original stays in online “vault”
 - Certified copy delivered on demand
 - No software or special knowledge req’d
 - Signature can be verified after printing
-
- Activity Log
 - Revision tracking
 - Password protection

Was it signed/sealed? **yes**
 Do we know the source? **yes**
 Is this the document? **yes**

Dear Client,

I issued this document through a trusted online registry which has verified my identity and holds the original safe from alteration.

The 12 digit document ID links to an online signature page where you (or anyone) can download a certified, watermarked copy at any time. The signature page shows my photo, contact and licensure information, as well as a description and thumbnail of the document.

Should any question arise as to the authenticity of this document, you can use the 12 digit ID (that shows on the face of the document even after printing) to download a fresh certified copy. Or you can contact me directly via the signature page.



Sincerely,

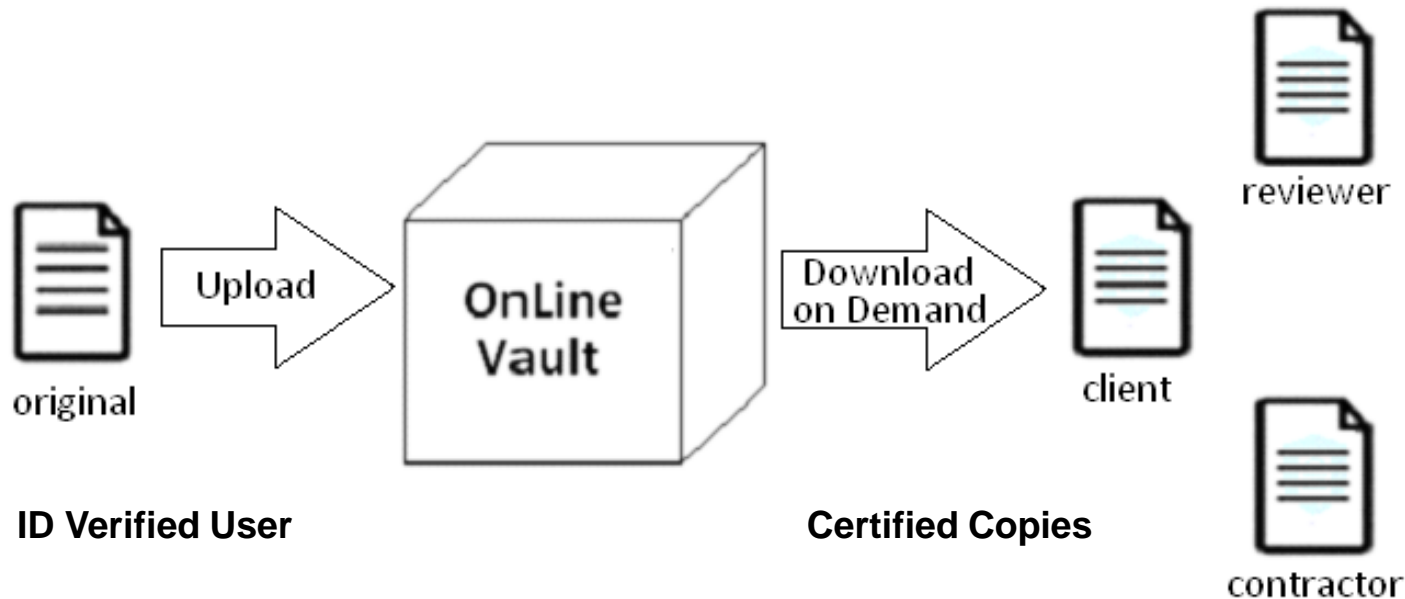
Peter McConaughy

Peter McConaughy, PE
Co-Founder

Digitally Signed: Thu, May 25, 2017 10:42 AM
 Downloaded: Wed, Jun 14, 2017 11:59 AM
 ID: 0b8bad1abd7c PRO Verified

Signature Options

5. SealAuthority – (Direct Document Delivery)




<https://sealauthority.com/documents/view/406e76e92af8>

Document is accessible to anyone who has the URL
 No opportunity for tampering in transit

Signature Options

5. SealAuthority Signature Page





Peter McConaughy
PRO Verified

Title: Structural Engineer

Discipline: Engineer ID Verified

Registration Number: 17795

McCon Engineering, Inc.
7214 New Cut Road
Kingville MD 21087
<http://www.McConEngineering.com>
mcoon@comcast.net
410-652-3635

Project: 15449 - Harf Co - Soma Barn

Project State: Maryland

Project Status: As Requested

Description:

Final walk-thru letter

Preview

Download

Document ID:
0b8bad1abd7c

Uploaded On: May 25, 2017

Filetype: pdf

Revision History

- This Document:
15449 - Final WalkThru

Summary

By signing a document, you accept professional responsibility for its content.

Your digital signature must do two things:



1. Prevent impostors from signing in your name, and



2. Prevent modification of the document after signing

Slide 27 of 31

Summary

Signature Options:	ID Verified?	TamperProof?
1. Wet Signature	yes	yes
2. E-signature	no	no
3. PKI (Self-Signed)	no	yes
4. PKI (Third Party)	yes	yes
5. SealAuthority	yes	yes

Q & A

Thank you!

Peter McConaughy, PE

410-652-3635

Peter@SealAuthority.com

www.SealAuthority.com



Slide 29 of 31

Going Digital: Digital Signatures & Digital Document Delivery

To receive credit for this course, each registrant will need to take the quiz below and pass with a score of 70 or above. Click link

<http://quiz.nspe.org/quiz/going-digital.aspx>

to take the quiz.

Going Digital: Digital Signatures & Digital Document Delivery

NSPE would like your feedback regarding this live webinar. Click link

<https://www.surveymonkey.com/r/588WM6R>

to take a short survey.