

DIGITAL SIGNATURES

CREATING AND VALIDATING SECURE ELECTRONIC DOCUMENTS

SECURING ELECTRONIC DOCUMENTS

- Digital signatures can be used by design professionals (Architects and Engineers) to authenticate the electronic documents they create for submittal to a permitting authority.
- This method of authenticating documents is authorized by the respective licensing boards by Administrative Rule
- Architects 61G1-16.005
- Engineers 61G15-23.003

61G1-16.005

- 61G1-16.005 Procedures for Signing and Sealing Electronically Transmitted Plans, Specifications, Reports or Other Documents.
- (1) Information stored in electronic files representing plans, specifications, plats, reports, or other documents which must be sealed under the provisions of Chapter 481, F.S., shall be signed, dated and sealed by the architect or interior designer in responsible charge.
- (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 61G1-16.003, F.A.C.

61G1-16.005

- (2) An architect or interior designer utilizing a digital signature to seal construction documents 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; and
- (d) Linked to a document in such a manner that the electronic signature is invalidated if any data in the document are changed.

61G15-23.003

- 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 "digital signature" and "electronic signature" shall have the meanings ascribed to them in Sections 668.003(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.

61G15-23.003

- (2) A professional engineer utilizing a digital signature to seal engineering work 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.

DIGITAL SIGNATURES

- A key point to remember is that a digital signature is only valid when the associated electronic document (digital file) can be authenticated with the signee's public key
- A paper printout of a digitally signed electronic document cannot be validated, and therefore cannot be used as an official record
- A digital signature must be created using key pair technology in accordance with the federal Secure Hash Standard also known as Federal Information Processing Standards, FIPS 180-3 or FIPS 180-4

HOW DIGITAL SIGNATURES WORK

- Digital signature technology is defined in Florida Statutes 668, using one of several algorithms to encode a signee's personal information, making it possible to authenticate the signature using the Encryption key produces
- PDF management software such as Adobe Acrobat or BlueBeam can be used to decode the signature, authenticate the signature and read the history of the file to determine if the file has been changed since the document was signed

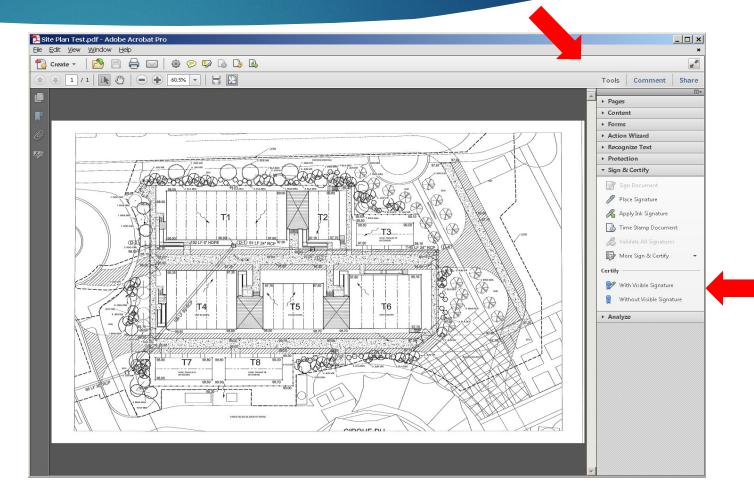
- ► As used in this act:
- (1) "Certificate" means a computer-based record which:
- (a) Identifies the certification authority.
- ▶ (b) Identifies the subscriber.
- ▶ (c) Contains the subscriber's public key.
- (d) Is digitally signed by the certification authority.

- (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

- (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.

To create a digital signature, open the "Tools" panel and select "Visual Signature"



Click on "OK" at the first screen

Save as Certified Document

(i)

You are about to create a certified document. By certifying a document, you vouch for its contents and enable recipients to verify that the document came from you. Certifying a document also adds tamper-resistance to detect and prevent unwanted changes.

To certify a document, you need to have a digital ID. If you intend to distribute this document to a large audience, it is suggested that you use a digital ID from one of Adobe's partners. This will allow any recipient with Acrobat or Adobe Reader to automatically verify the certification.

Get Digital ID from Adobe Partner...

🔲 🗋 Don't show again



OK

X

Help

CREATE A SIGNATURE

 Click "OK" to create a signature field.

Do <u>n</u> ot show this message again OK Cancel	Adobe	Acrobat To create a signature field, first click OK to close this dialog, then click and drag out the field's area in the location where it should appear in the document. After creating the signature field, you'll be asked to choose additional options to complete signing.

- After the signature field is created the signature file can be selected, or a new signature can be created.
- Note that you only have to signature file is created a signature once
- Select "New Digital ID" to create your signature

Add Digital ID

Add or create a digital ID to sign and encrypt documents. The certificate that comes with your digital ID is sent to others so that they can verify your signature. Add or create a digital ID using:

×

Next >

< Back

O My existing digital ID from:

 \bigcirc A file

Cancel

- O A roaming digital ID accessed via a server
- O A device connected to this computer

A new digital ID I want to create now

BOAF / AIA-FLORIDA / FES JOINT TASK FORCE

Fill in all of the open fields and click "Finish"

ld Digital ID				×
Enter your identity inform certificate.	nation to be used wh	ien generating t	he self-signed	
Na <u>m</u> e (e.g. John Smith):				
Organizational <u>U</u> nit:				
Organization Name:				
<u>E</u> mail Address:				
<u>C</u> ountry/Region:	US - UNITED STAT	ES	•]
En <u>a</u> ble Unicode Suppo	ort			
Cancel		< <u>B</u> ack	<u>E</u> inish]

To create a password protected Digital ID select "New PKCS#12 digital ID File" and click Next

Add Digital ID

Where would you like to store your self-signed digital ID?

New PKCS#12 digital ID file



Creates a new password protected digital ID file that uses the standard PKCS#12 format. This common digital ID file format is supported by most security software applications, including major web browsers. PKCS#12 files have a .pfx or .p12 file extension.

O Windows Certificate Store

Your digital ID will be stored in the Windows Certificate Store where it will also be available to other Windows applications. The digital ID will be protected by your Windows login.

| <u>N</u>ext >

< <u>B</u>ack

X

- ▶ The file name will pre-load
- Create a password and confirm
- Click "Finish"

ld Digital ID	×
Enter a file location and password for your new digital ID file. You will need the you use the digital ID to sign or decrypt documents. You should make a note o so that you can copy this file for backup or other purposes. You can later chang file using the Security Settings dialog.	f the file location
Fjle Name:	
C:\JohnO'Connor.pfx	B <u>r</u> owse
Password:	
<u>C</u> onfirm Password:	
Cancel < <u>B</u> ack	Einish

- Now your digital ID has been created and can be used to certify the document
- The top line is your signature file name; It will auto-load
- On the second line fill in your password
- The third line is the name of the visible signature, it will auto-load
- The fourth line will auto load the signature info

ertify Document	l
Sign As: John O'Connor <joconnor@rcid.org> 💽 🧕</joconnor@rcid.org>	
Password:	
Certificate Issuer: John O'Connor I <u>n</u> fo	
Appearance: John O'Connor 💌	
Certified by John O'Connor DN: cn=John O'Connor, o=RCID, ou=Building and Safety, email=joconnor@rcid.org, c=US Date: 2013.06.27 11:28:19 -04'00'	-
Per <u>m</u> itted Actions After Certifying	
Annotations, form fill-in, and digital signatu	
No changes allowed Form fill-in and digital signatures	
Annotations, form fill-in, and digital signatures Cancel	

Open the drop-down list and select choose new Appearance

Certify Document
Sign As: John O'Connor <joconnor@rcid.org> 💽 🙍</joconnor@rcid.org>
Password:
Certificate Issuer: John O'Connor I <u>n</u> fo
Appearance: John O'Connor
Cortified by John O'Connor
Certate New Appearance ou=Building and Safety, email=joconnor@rcid.org, c=US Date: 2013.06.27 11:28:19 -04'00'
Per <u>m</u> itted Actions After Certifying
No changes allowed
Sign Cancel

- Name the signature
- Edit the fields as needed
- Import an image

itle: John O'Connor	
Preview	
Digitally signed by your common name DN: your distinguished name here Reason: your signing reason here Location: your signing location here Date: 2013.06.18 12:01:00 -04'00'	here
Configure Graphic	
Show: O No graphi <u>c</u> Import Graphic from:	
Imported graphic <u>Eile</u>	
○ Name	
Configure Text	
Show: 🔽 Name 💌 Location 🔽 Distinguished name 💌	Logo
☑ Date ☑ Reason ☑ Labels	
Text Properties	
Text Direction: Auto Left to right Right to left 	
Digits: 0123456789	
OK	Cancel

 Before the signature is added the file must be saved

🔁 Save As		×
Savejn:	📔 Certificate Tests 🔄 🕑 🧭 🖽 🗸	
	Name 🔺 🚽 Date modified 🔽 Type 🔽 Size 🔺	
	Site Plan Test v3 signed 06/18/2013 12:5 Adobe Acrobat	
Recent Places	Site Plan Test V4 signed 06/18/2013 12:5 Adobe Acrobat	
	Site Plan Test 06/20/2013 4:29 Adobe Acrobat	
	Splitsville 4 Lane Short Lane Miami (B mor 02/14/2013 9:47 Adobe Acrobat	
Desktop	Splitsville-DTD_FA AsBuilds_Certified 02/14/2013 9:47 Adobe Acrobat	
<u> </u>	Test PDF JLO Signed 06/18/2013 12:2 Adobe Acrobat	
	Test PDF JLO v2 06/20/2013 4:45 Adobe Acrobat	
Libraries	Test PDF JLO v3 06/20/2013 4:48 Adobe Acrobat Image: Comparison of the second seco	
	Test PDF JLO v4 06/27/2013 8:10 Adobe Acrobat Image: Comparison of the second seco	
	Test PDF JLO v5 06/27/2013 10:2 Adobe Acrobat	
Computer	Test PDF JLO v6 06/27/2013 10:3 Adobe Acrobat Image: Comparison of the second seco	
<u> (11)</u>	Test PDF JLO v7 06/27/2013 11:2 Adobe Acrobat Image: Comparison of the second seco	
	Test PDF JLO 06/18/2013 11:4 Adobe Acrobat Image: Comparison of the second	
Network	12 v7 06/27/2013 11:1 Adobe Acrobat	
	File name: Test PDF JLO v8	
	Save as type: Adobe PDF Files (*.pdf)	

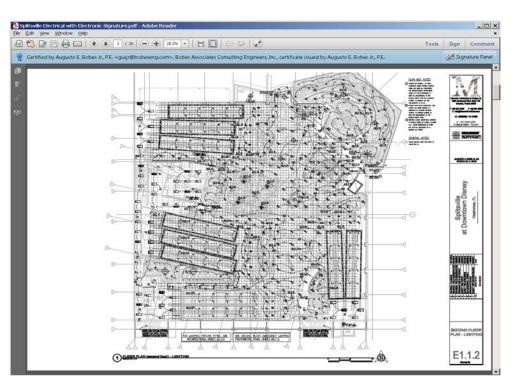
 Before the signature is added the file must be saved

🔁 Save As		×
Savejn:	📔 Certificate Tests 🔄 🕑 🧭 🖽 🗸	
	Name 🔺 🚽 Date modified 🔽 Type 🔽 Size 🔺	
	Site Plan Test v3 signed 06/18/2013 12:5 Adobe Acrobat	
Recent Places	Site Plan Test V4 signed 06/18/2013 12:5 Adobe Acrobat	
	Site Plan Test 06/20/2013 4:29 Adobe Acrobat	
	Splitsville 4 Lane Short Lane Miami (B mor 02/14/2013 9:47 Adobe Acrobat	
Desktop	Splitsville-DTD_FA AsBuilds_Certified 02/14/2013 9:47 Adobe Acrobat	
<u> </u>	Test PDF JLO Signed 06/18/2013 12:2 Adobe Acrobat	
	Test PDF JLO v2 06/20/2013 4:45 Adobe Acrobat	
Libraries	Test PDF JLO v3 06/20/2013 4:48 Adobe Acrobat Image: Comparison of the second seco	
	Test PDF JLO v4 06/27/2013 8:10 Adobe Acrobat Image: Comparison of the second seco	
	Test PDF JLO v5 06/27/2013 10:2 Adobe Acrobat	
Computer	Test PDF JLO v6 06/27/2013 10:3 Adobe Acrobat Image: Comparison of the second seco	
<u> (11)</u>	Test PDF JLO v7 06/27/2013 11:2 Adobe Acrobat Image: Comparison of the second seco	
	Test PDF JLO 06/18/2013 11:4 Adobe Acrobat Image: Comparison of the second	
Network	12 v7 06/27/2013 11:1 Adobe Acrobat	
	File name: Test PDF JLO v8	
	Save as type: Adobe PDF Files (*.pdf)	

VALIDATING A SIGNATURE

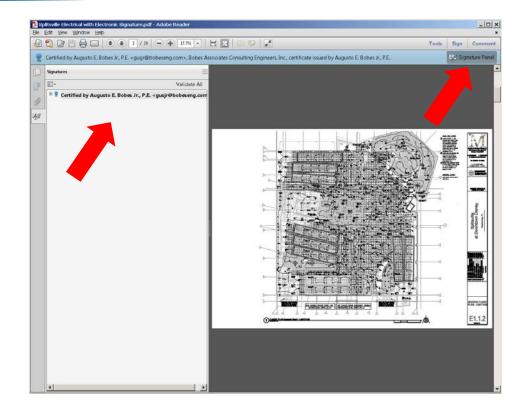
The most commonly used PDF reader is ADOBE Arobat. With their free PDF reader it is possible to view file content, see the document history and validate digital signatures

When a drawing file is opened with Adobe Acrobat, the program will indicate if it has been digitally signed by showing the signature panel button in the right side of the tray above the drawing



VALIDATING A SIGNATURE

- Click on the Signature Panel button to open the signature panel
- The name of the signee will be shown



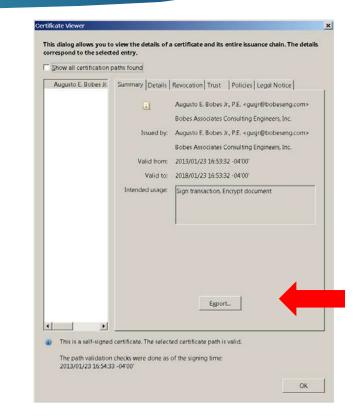
VALIDATING A SIGNATURE

From the Signature Properties panel click on the Show Certificate button

Signature Properties	×
Document certification is valid, signed by Augusto E. Bobes Jr., P.E. gusjr@bobeseng.com>. Summary Document Signer Date/Time Legal	1
Signed by: bes Jr., P.E. <gusjr@bobeseng.com> Show Certificate Reason: Not available</gusjr@bobeseng.com>	
Signing Time: 2013/01/23 16:54:33 -04'00' Location: Not available	
Validity Summary	
😚 The Document has not been modified since it was certified.	
The signer's identity is valid.	
Signing time is from the clock on the signer's computer.	
Signature was created using Adobe Acrobat 9.2.0. Signature was validated as of the signing time: 2013/01/23 16:54:33 -04'00'	
<u>⊻</u> alidate Signature <u>C</u> lose	1

BOAF / AIA-FLORIDA / FES JOINT TASK FORCE

- The signee must send the public key to the Authority Having Jurisdiction
- This is done by exporting the public key
- The Authority Having Jurisdiction must receive the public key and save it in the adobe trusted certificate folder



Click on the Export the encrypted data line and then the next button

ata Exchange File - Exporting Certificate		×
 Choose Export Options Identity Sign Data Exchange File Create Email Contents Review and Complete 	You have chosen to export the following data: Selected address book entries To open the exported data, you need Adobe Acrobat 6.0 Professional or Standard, Adobe Reader 6.0, or later versions. Destination © Email the exported data © Save the exported data to a file © Acrobat FDF Data Exchange © Certificate Message Syntax - PKCS#7 © Certificate File	
	Cancel Sack Next >	j

Fill in the information and click the next button

Steps	
Choose Export Options Identity Sign Data Exchange File 	Your identity information is used with comments, reviews, and digital signatures. Information entered here is secure and not transmitted beyond this application without your knowledge. To modify this information in the future, simply go to the Identity panel in the preferences.
Create Email Contents Review and Complete	Identity Login Name: Name: Iitle: Iitle: Organization Name: Organization Unit: Email Address:

Skip the sign the file option and click next

In Data Exchange File ignature If you intend to share this data with someone else, you may want to Sign	_
digitally sign the data so that the recipient can verify where it came	
	:ancel

Address the file to the Authority Having Jurisdiction and click next

Choose Export Options	You can specify the contents of the email message to which you will attach the exported data. This information will be sent to your email program.
Identity	-Morrago
Sign Data Exchange File	Message
	Io:
Create Email Contents	
Review and Complete	Subject: Acrobat FDF Data Exchange File
	Attached is an Acrobat FDF Data Exchange File.
	The attached file contains a list of certificates that you can use to validate signatures and encrypt documents.
	Opening this file will start Adobe Acrobat or Adobe Reader and prompt you to process the file.
	To open and process the file attachment, you need Adobe Acrobat 6.0 Professional
	or Standard, Adobe Reader 6.0, or later versions.

TRUSTING A CERTIFICATE

- Select the Trust tab and check all of the trust settings
- Click on the trust button

usto E. Bobes Jr. Summary Details Revocation Trust Policies Legal Notice This certificate is directly trusted in your trusted identities list. Trust Settings This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to: Sign documents or data Certify documents Execute high privilege JavaScripts that are embedded in a certified document Execute high privilege JavaScripts that are embedded in a certified document Perform privileged system operations (networking, printing, file access, etc.) Add to Trusted Identities.	This certificate is directly trusted in your trusted identifies list. Trust Settings This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to: Sign documents or data Certify documents Execute dynamic content that is embedded in a certified document Execute high privilege JavaScripts that are embedded in a	
 Trust Settings This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to: Sign documents or data Certify documents Execute dynamic content that is embedded in a certified document Execute high privilege JavaScripts that are embedded in a certified document Perform privileged system operations (networking, printing, file access, etc.) 	Trust Settings This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to: Sign documents or data Certify documents Execute dynamic content that is embedded in a certified document Execute high privilege JavaScripts that are embedded in a	
 This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to: Sign documents or data Certify documents Execute dynamic content that is embedded in a certified document Execute high privilege JavaScripts that are embedded in a certified document. Perform privileged system operations (networking, printing, file access, etc.) 	This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to: Image: Sign documents or data Image: Certify documents Image: Certify documents Image: Execute dynamic content that is embedded in a certified document Image: Execute high privilege JavaScripts that are embedded in a	
 certificate and all certificates issued beneath this certificate are trusted to: Sign documents or data Certify documents Execute dynamic content that is embedded in a certified document Execute high privilege JavaScripts that are embedded in a certified document. Perform privileged system operations (networking, printing, file access, etc.) 	 certificate and all certificates issued beneath this certificate are trusted to: Sign documents or data Certify documents Execute dynamic content that is embedded in a certified document Execute high privilege JavaScripts that are embedded in a 	
 Certify documents Execute dynamic content that is embedded in a certified document Execute high privilege JavaScripts that are embedded in a certified document. Perform privileged system operations (networking, printing, file access, etc.) 	Certify documents Execute dynamic content that is embedded in a certified document Execute high privilege JavaScripts that are embedded in a	
 Execute dynamic content that is embedded in a certified document Execute high privilege JavaScripts that are embedded in a certified document Perform privileged system operations (networking, printing, file access, etc.) 	 Execute dynamic content that is embedded in a certified document Execute high privilege JavaScripts that are embedded in a 	
document Execute high privilege JavaScripts that are embedded in a certified document Perform privileged system operations (networking, printing, file access, etc.)	document Execute high privilege JavaScripts that are embedded in a	
certified document Perform privileged system operations (networking, printing, file access, etc.)	Execute ingit privilege seressing of the entreespeering	
printing, file access, etc.)	certified document	
Add to Trusted Identities	i alterni printaga a system a paratari i paratari g	
	Add to Trusted Identities.	

BOAF / AIA-FLORIDA / FES JOINT TASK FORCE

TRUSTING A CERTIFICATE

- Check the content boxes
- Click on the Ok button

Subject: Raymond Schaefer <rschaefer@maverickarchdes.com></rschaefer@maverickarchdes.com>
Issuer: Raymond Schaefer <rschaefer@maverickarchdes.com></rschaefer@maverickarchdes.com>
Usage: Sign transaction, Encrypt document
Expiration: 02/14/2018 5:25:09 PM
Trust
A certificate used to sign a document must either be designated as a trust anchor or chain up to a trust anchor in order for signature validation to succeed. Revocation checking is not performed on or above a trust anchor. Use this certificate as a trusted root If signature validation succeeds, trust this certificate for:
Signed documents or data
Certified documents
Dynamic content
Embedded high privilege JavaScript
Help OK Cancel

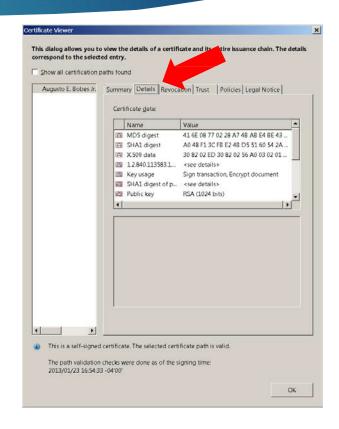
×

mport Contact Settings

Certificate Details

VIEWING SIGNATURE DETAILS

Open the Details tab to view information about the signature



VIEWING SIGNATURE DETAILS

Move the slide down to view more information

ert	ific	at	e V	ie	we

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

Show all certification paths found

	Name	Value	-
iii	Validity ends	2018/01/23 16:53:32 -04'00'	
8	Validity starts	2013/01/23 16:53:32 -04'00'	
8	Serial number	4A 22 BB F1 3E E0 01 35 0D 2E	
8	S Issuer	c=US, email=gusjr@bobeseng.com, o	
192	Subject	c=US, email=gusjr@bobeseng.com, o	
8	Signature algorit	SHA1 RSA	
12	Version	3	-
1		•	
			_
×			
	cate. The selected cert	ificate path is valid	

VIEWING SIGNATURE DETAILS

The public key can be seen by highlighting the Public Key line

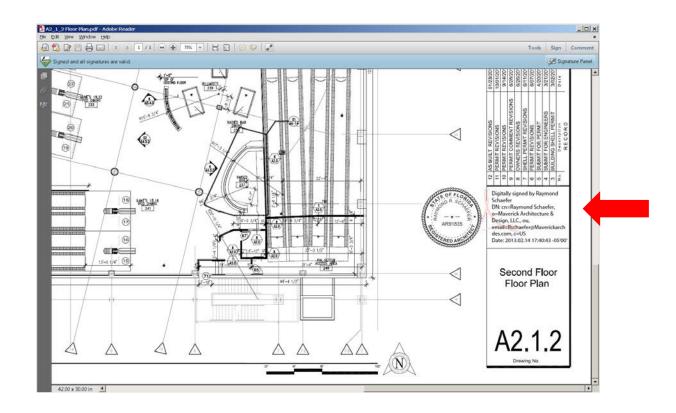
	Name	Value	-
	12.840.113583.1	<see details=""></see>	- (A)
2	Key usage	Sign transaction, Encrypt document	111
22	SHA1 digest of p	<see details=""></see>	
123	Public key	RSA (1024 bits)	
83	Validity ends	2018/01/23 16:53:32 -04'00'	_
100	Validity starts	2013/01/23 16:53:32 -04'00'	
100	Serial number	4A 22 88 F1 3E E0 01 35 0D 2E	+
4			•
00 0 6F 3	5 29 7C 52 D2 4E 36 5 08 B3 88 54 83 F1	9 63 1B 2B 44 68 AF BC 2E CD 1F 18 F0 09 41 43 6F 5F A7 C1 1B 52 0C 7F 41 F3 D7 54 91 95 F7 BE BB 1E 68 0C 38 E4 22 1D7 2C 84 C5 A3 39 2F F6 6F 15 94 38 9	A1 81
00 0 6F 3 6C 5	5 29 7C 52 D2 4E 36 5 08 B3 88 54 83 F1	09 41 43 6F 5F A7 C1 1B 52 0C 7F 41 F1 D7 54 91 95 F7 BE 8B 1E 68 0C 38 E4 28 8 D7 2C 84 C5 A3 39 2F E6 6F 15 94 38 9	A1 81
00 0 6F 3 6C 5	5 29 7C 52 D2 4E 36 5 08 B3 88 54 83 F1 52 89 AE B3 FC CC 23	09 41 43 6F 5F A7 C1 1B 52 0C 7F 41 F1 D7 54 91 95 F7 BE 8B 1E 68 0C 38 E4 28 8 D7 2C 84 C5 A3 39 2F E6 6F 15 94 38 9	A1 81

This dialog allows you to view the details of a certificate and its entire issuance chain. The details

and to the selected entry.

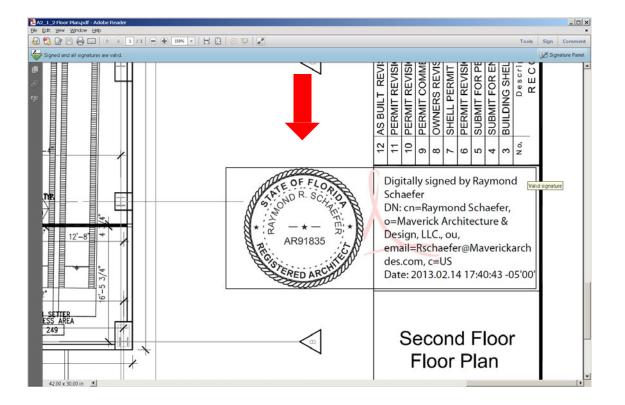
VISIBLE SIGNATURE IMAGES

- A visible signature image is not required in the validation process
- However, a visible signature image created by the signature software is helpful to notify the reviewer that the document is digitally signed
- A visible signature will contain information required by the rules



VISIBLE SIGNATURE IMAGES

A proper visible image can include an image of the signee's seal, the name of the signee, date, contact information, and the phrase "Digitally signed by..."



THANK YOU FOR ATTENDING







BOAF / AIA-FLORIDA / FES JOINT TASK FORCE