

*State of Florida
Department of Transportation*



FDOT Digital Delivery

CE-11-0136

User Training Manual

January 13, 2016

ENGINEERING / CADD SYSTEMS OFFICE

TALLAHASSEE, FLORIDA

<http://www.dot.state.fl.us/ecso/>

FDOT Digital Delivery

CE-11-0136

Description

This training manual is designed to

- Equip professionally registered individuals, design professionals and those involved in the Florida Department of Transportation (FDOT) design, plans delivery & construction process with skills necessary to use digital certificates for signing and validating contract documents,
- Eliminate the need to scan paper documents for signature approvals,
- Create a seamless process for contract documents from concept through construction,
- Provide a means for chain of possession / chain of approval for documents,
- Present options for popular software used to sign PDF and delivery options using Portable Document Format (PDF) Portfolio.

Objectives

On completion of this course students will know and understand:

- The basics of how to acquire and manage a Digital Certificate.
- What is ACES policy?
- How to create a Digital Signature appearance.
- The requirements of Florida Administrative Code regarding Digital Signature.
- FDOT Digital Delivery Process:
 - File Naming structure and Project organization
 - Single & Multiple Signatories on plan sets
 - Authentication and Validation
 - Revisions, Deliverables & Digital Signature Delivery
 - What is & What is not Required
- Signing documents other than Contract Plan Sets

Audience

Professionally registered Architects, Engineers and Surveyors who will apply their professional seal to documents. Design professionals who produce or approve documents. Management professionals for whom Digital Signature alters their business model. IT personnel who support the Digital Signature effort.

Prerequisites

Students must have a basic understanding of the FDOT design and delivery process. Must have computer skills necessary to organize files and folders and operate a windows base operating system. Some understanding of PDF and how it is produced.

Duration: 4 Hours

Professional Credit Hours: 4 PDHs

Table of Contents

1	FIRST STEPS	1-1
	ACQUIRE A DIGITAL CERTIFICATE	1-1
	<i>FDOT Employees:</i>	1-1
	<i>Non – FDOT Personnel</i>	1-2
	<i>Identity Vetting</i>	1-3
	INSTALLATION & MANAGEMENT	1-3
	<i>Current Installations</i>	1-4
	<i>Installation</i>	1-5
	Exporting - Backups	1-5
	Importing a Certificate	1-5
	Certificate Lost or Compromised	1-6
	OIT - STANDARDS	1-6
2	DOCUMENT SIGNING	2-1
	THE APPEARANCE	2-1
	<i>Adobe</i>	2-1
	<i>BlueBeam</i>	2-3
	SIGNING A DOCUMENT	2-4
	<i>Click and Drag – The Quick and dirty method</i>	2-4
	<i>Using Signature blocks</i>	2-4
	<i>Certifying the Document</i>	2-5
	<i>Signing and Linking Multiple Documents</i>	2-6
	FLORIDA ADMINISTRATIVE CODE REGARDING DIGITAL SIGNATURE	2-6
3	FDOT DIGITAL PRODUCTION & DELIVERY	3-1
	PROJECT PRODUCTION	3-1
	<i>Project Creation</i>	3-1
	PROJECT DELIVERY	3-5
	<i>Plan Sets by Component</i>	3-6
	<i>Early Work</i>	3-6
4	OTHER TYPES OF DOCUMENTS	4-1
	MICROSOFT OFFICE SUITE	4-1
	DATA TYPES TO BE DELIVERED	4-3
	<i>XML Signing</i>	4-4

1 FIRST STEPS

ACQUIRE A DIGITAL CERTIFICATE

Florida Department of Transportation (FDOT) employees have a specific means for acquiring a digital certificate. This is originated using the Automated Access Request Form (AARF) system. Non-FDOT personnel can acquire their certificates directly from a Certificate Authority (CA).

FDOT EMPLOYEES:

1. Navigate to <http://infonet/>. Non – FDOT personnel skip ahead to next section.

Home | Agency Directory | Internet | Offices | Search

Central FDOT INFONET 1915 & 2015

Agency Resources
[Awards and Special Events](#)
[Emergency Information](#)
[Executive Meetings](#)
[Executive Management Team](#)
[Forms, Policies and Procedures](#)
[Historical Archive](#)
[Mission, Vision, Values](#)
[Organizational Chart](#)
[Organizational Development](#)
[Templates and Images](#)
[Training and Development](#)

Secretary's Corner
[Innovators! Team](#)
[Secretary's Challenge](#)
[Suggestion Box](#)
[Town Hall Webinar](#)

Latest From Twitter
Tweets from
<https://twitter.com/MyFDOT/lists/fdot-central-office>

TRANSPORTATION INNOVATION CHALLENGE

Transportation Innovation Challenge - FDOT continually strives to enhance all areas of our operations. We invite you to share your thoughts on ways that we can challenge ourselves to be innovative, efficient and exceptional – [Submit Your Idea](#)

Employment
Insurance and Benefits
Job Vacancies
Payroll Information
People First Resources
State Holidays
More...

News
Daily Clips / DOTNEWS
FDOT / District Newsletters
OIG Examiner
Safety Advisor
Security Newsline
More...

Technology
Application / Web Development
E-Mail / File Sharing
Enterprise Applications
Enterprise Information Portal
Mainframe
More... (0.365 Help)

Other Resources

Business
[Contracts/Services](#)
[Purchasing Card](#)
[State Contract Search](#)
[Travel](#)
[Work Activity Codes](#)
[More...](#)

E-Forms
[Computer Access \(AARF\)](#)
[Computer Software \(IRR\)](#)
[Correspondence \(FDOTracker\)](#)
[Publications Registry](#)
[Public Meeting Notices](#)
[More...](#)

Legal
[Claims](#)
[Contacts](#)
[FL Administrative Code](#)
[Florida Statutes](#)
[Public Records](#)
[More...](#)

Legislative
[Contacts](#)
[Current Legislation](#)
[Legislative Overview](#)
[State Legislators](#)
[State Representatives](#)
[More...](#)

Start with AARF

Central | District 1 | District 2 | District 3 | District 4 | District 5 | District 6 | District 7 | Turnpike
FDOT Service Desk: 866-955-HELP (4357) | E-Mail Us | Website
Hours: Monday to Friday 7:00 a.m. to 5:30 p.m. (EST)

2. Click “Computer Access (AARF)”, you should see the following Automated Access Request Form dialog.

Automated Access Request Form

Home Create Request Pending Requests Search

Welcome to the Florida Department of Transportation

This system was designed to provide a secure, statewide computer security system that can quickly respond and coordinate with other systems. Strict guidelines must be followed to ensure the security of the diverse systems, which are critical to the state's operations. If you need to request access to a system, please select the appropriate request type.

-- Computer Security Team

New User / Account
Name Change
Access Change
Transfer
Termination
Other Request Types

3. Once inside the AARF System select **Create Request**. This will present a drop-down menu.
4. From the menu select **Access Change**.
5. Once in the **Access Change** dialog, complete the required field to search for the individual changing their access. Input both *First Name* and *Last Name* <or> input *User ID* and click **Find**.
6. This will produce a list of individuals who match the search criteria. If the correct name is in the list (it may be a list of only one) click **Use and Continue**.
7. Next there will be a screen with the user's personal information. Ensure that the correct individual was selected and click **Continue**. This will present a screen with all of the access granted for that user.
8. Scroll down until the check box labeled "**Digital Signature Certificate**" is visible. Check the box.

<input type="checkbox"/> Cost Analysis	<input type="checkbox"/> FACTS
<input type="checkbox"/> Density Log (DL) Citrix	<input type="checkbox"/> FAMS - Federal Authc James Jobe or Sean McA
<input checked="" type="checkbox"/> Digital Signature Certificate	<input type="checkbox"/> FIRM - Facilities Inv R
<input type="checkbox"/> EDMS - Loading DOC (Business Area)	<input type="checkbox"/> FLAIR
<input type="checkbox"/> EDMS - Loading DOC (User Role)	<input type="checkbox"/> FLAIR Additional Prop

9. Once the box is checked, scroll down near the bottom and click **Continue**. This action will start a chain of notifications by email to the supervisor for the individual, the cost center manager and Office of Information Technology (OIT).
10. Once the proper approvals are in place. The individual will receive notification of approval to acquire a *Digital Certificate*. This notification includes an *order number*. This order number is used as a method of payment on the *Identrust* website. The cost is covered and does not come from the individuals cost center.

NON – FDOT PERSONNEL

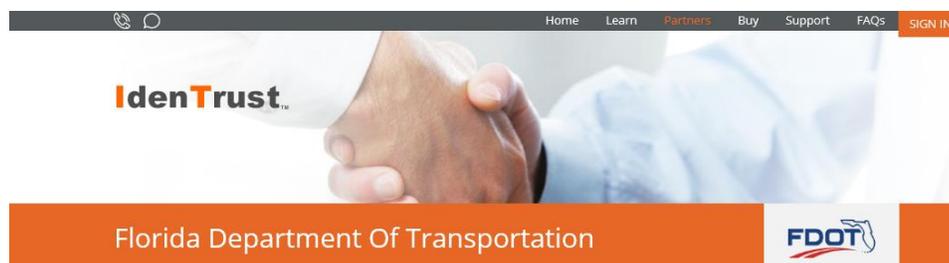
Individuals who do business with the FDOT have a few options as far as which digital certificate they use. A list of digital certificate authorities approved for use by the FDOT can be found at the following address:

<http://www.dot.state.fl.us/OIS/ApprovedDigitalCertificateAuthorities.shtm>

Check cost and what is included with the certificate; such as, software, user support, etcetera. Ensure that the certificate that you get is used for *document signing*. There are many different types of certificate, ensure that you get the right one. The one used internally at FDOT is *Identrust*.

To acquire a certificate from *IdenTrust* for doing business with FDOT navigate to the following site:

<http://www.identrust.com/fdot/index.html>



Read carefully the section on *Professional Licensure Digital Signing and Sealing*. Subscribers to digital certificates must have exclusive use. The certificate must be in their sole control and possession. Select the certificate that is appropriate for you.

Important! *FDOT Personnel, ensure that you get the Business Representative.*

ACES Digital Certificate:

Access Certificates for Electronic Services (ACES)

CERTIFICATE TYPE	SUBSCRIBER	PURPOSE/USAGE	COST
Business Representative	Employee authorized to act on behalf of a company	Identity Authentication Digital Signature/Signing Usage: authenticate yourself as an employee (affiliated) of a valid business when signing emails and documents, and identifying yourself to gain access to restricted web sites.	\$119.00 two years + Hardware <input type="button" value="buy"/>
Unaffiliated Individual	Individual representing him/herself	Individual Certificates are sold to those who are acting as representatives of themselves, not on behalf of a company. If you are a sole proprietor and wish to have your identity authenticated independently from your company, <i>more personal information is required</i> , including social security number, credit card number, driver's license number, and home phone number.	\$75.00 two years + Hardware <input type="button" value="buy"/>

For complete instructional videos navigate to Engineering/CADD Systems Office (ECSSO) Posted Webinars website under the category FDOT General Resources:

<http://www.dot.state.fl.us/ecso/downloads/webinars/Posted.shtm>

and expand the section FDOT Digital Delivery.

IDENTITY VETTING

The confirmation process for truth of an individual's identity claim:

http://www.identrust.com/support/aces_support.html

INSTALLATION & MANAGEMENT

Digital certificates can reside on a number of different media. Hardware certificates can reside on a USB device or a Near Field Communication (NFC) device; this is usually some type of smart card with a chip. The type of certificates the FDOT is using are software certificates. On the Windows operating system these reside in the registry.

Due care must be taken to insure that the private keys always remains in the direct control of the subscriber! This information is the personal identity of the subscriber and should be handled with due care as one would handle bank account numbers, credit card numbers, and the like. It is recommended that the certificate be on a workstation that the subscriber has access to and perhaps one mobile device, laptop computer.

Also, it is recommended that a backup be held in a secure location by the subscriber.

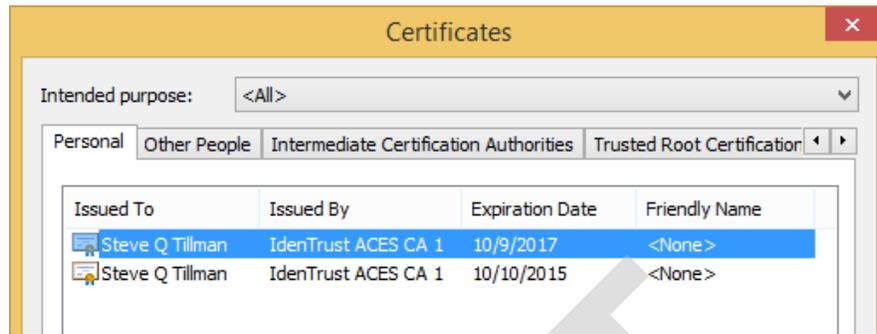
UNDER NO CIRCUMSTANCES IS THE CERTIFICATE & PRIVATE KEY SHARED OR THE PASSWORD REVEALED FOR USE BY ANOTHER. THE SUBSCRIBER OF THE CERTIFICATE MUST HAVE SOLE CONTROL OF THE DIGITAL CERTIFICATE AT ALL TIMES.

If the certificate is not under the sole control of the subscriber it must be revoked, as this is a violation of the certificate agreement and FDOT policy.

CURRENT INSTALLATIONS

Before installing, exporting or removing certificates, it is best to see what certificates already exist on the workstation. There are a couple of different ways to do this. Using the Windows Internet Explorer menu bar, select **Tools > Internet Options**. The Internet Options dialog will display. From the tabs along the top of the dialog select **Content > Certificates**. You should see a similar **Certificates** dialog.

Note If your Windows Internet Explorer does not have a menu bar, right click at the top of the browser and select Menu Bar from the drop-down menu.



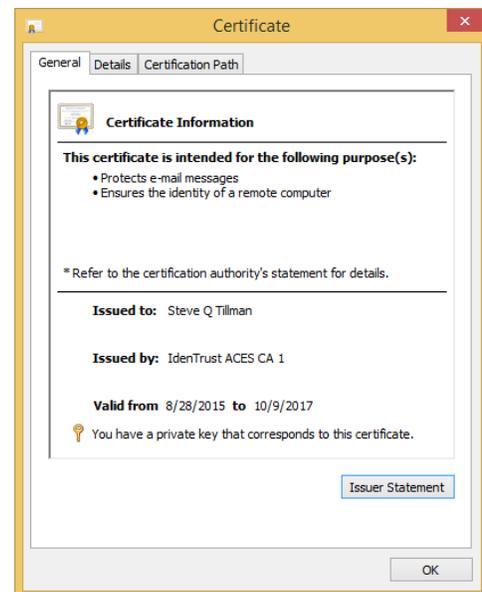
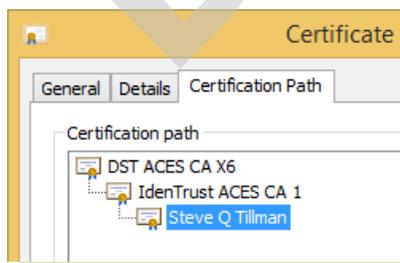
The *Personal* tab displays your personal certificates. The details about a specific certificate can be viewed by selecting the certificate and clicking the **View** button to display a **Certificate** dialog of the certificate selected.

Some of the certificates in this list may be beyond their validity period; they may be expired. Do not remove certificates from this list unless you are very certain about what you are doing; there may be unintended consequences. Certificates listed here may be used by other applications for client authentication, securing email, securing data and access to various network services. Inadvertently removing one could result in a lack of service.

From the specific **Certificate** dialog under the *General* tab, the intended purpose for the certificate is to display the personal information of whom it was issued and by whom. The validity period, from and to dates, is also shown along with a private key associated with the certificate.

The next *Details* tab displays the detailed information about the certificate.

The last tab shows the *Certificate Path*.



Certificates issued by a certificate authority come bundled with intermediate and root certificates. The root certificate is used to sign the intermediate certificate, the intermediate is used to sign the personal certificate. The certificate has an ancestry; this is called a certificate path.

- The top level or *Root Certificate* is found in your *Trusted Root Certification Authorities* tab,
- The middle level or *Intermediate Certificate* is found under the *Intermediate Certification Authorities* tab,
- Finally your *Personal Certificate* is found under the *Personal* tab.

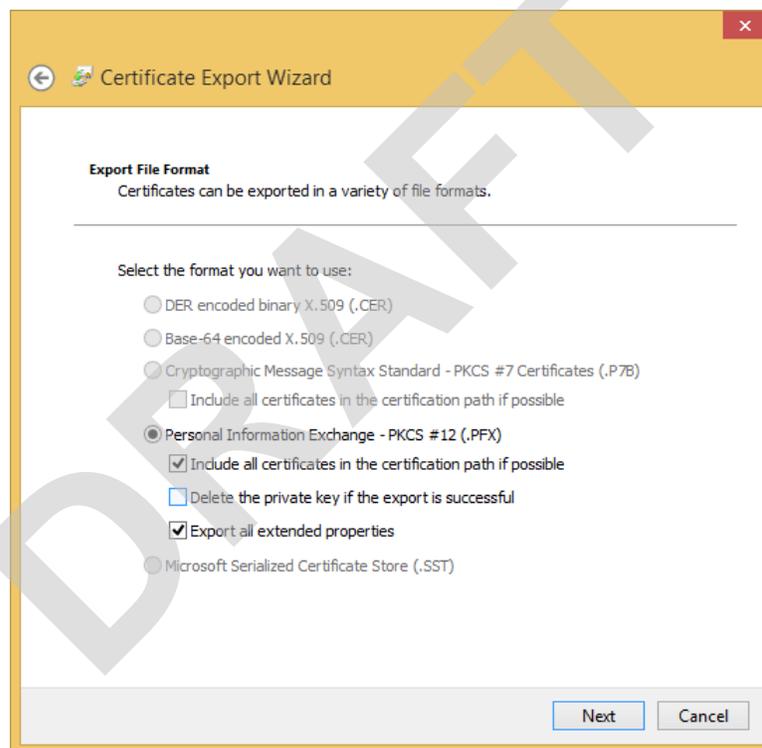
All certificates from a particular CA will be issued under the same Root Certificate. Therefore by trusting the Root Certificate all descendants are trusted.

INSTALLATION

Most certificate authorities have an automated process on their website that installs a certificate. This is the simplest and easiest way to install. However there may be instances where a certificate must be install manually. This is usually the case where a certificate is moved from one computer to another or is being restored from a backup.

EXPORTING - BACKUPS

1. From the **Certificates** dialog, click the **Export** button. This will bring up the **Certificate Export Wizard** dialog.
2. Exporting creates a copy and places it elsewhere, leaving the initial certificate intact. Click **Next** to get started.
3. The first dialog asks if the *private key* is to be exported along with the certificate; click **Yes**. The private key is used to sign a document, without it there will be no document signing. The *private key password* is needed to export the private key.
4. Click **Next** to bring us to the *Export File Format* as seen below.



5. The only choice here is a Personal Information Exchange file in PKCS12 format. The file will have a .PFX file extension. Select the boxes as shown above and click **Next** for the Security options. If you are given the option, use a group or user name to secure the private key. This will prevent unintended individuals from installing the exported certificate elsewhere.

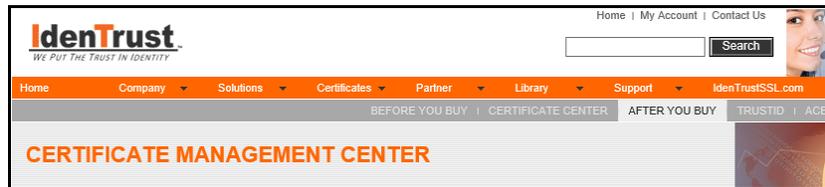
IMPORTING A CERTIFICATE

To import a certificate double left-click the file. Usually the certificates are transported in files in one of a number of different formats; CER, P7B, or PFX. The windows operating system will recognize the file as a certificate and open the Certificate Import Wizard. The CER format contains a single encoded certificate. The other formats contain a certificate chain that are logically linked together and may or may not contain a private key. Private keys are password protected, so a password will be needed to install them. This is commonly known as a certificate bundle.

CERTIFICATE LOST OR COMPROMISED

The Certificate management center.

http://www.identrust.com/certificates/cert_management_center.html



On this web site, using IdenTrust account login credentials certificate holders can do the following:

- Renew a certificate if it is within 90 days of expiration.
- Revoke a certificate if information contained in it is no longer accurate or the private key has been lost or compromised.
- Update your contact information if certificate holder has moved or would like to change contact phone number or e-mail address.
- Recover an encryption certificate (requires entering account number IdenTrust\DST passphrase)

Also there is live chat available for other unanswered questions.

STOP: Lab 1

OIT - STANDARDS

The Office of Information Technology has published two chapters in their OIS Manual regarding the acquisition & use of digital signatures at FDOT (effective January 8, 2016).

<http://www.dot.state.fl.us/OIS/OISManual.shtm>

CHAPTER 21 - Acquiring and Managing Digital Certificate addresses the procedure.

This chapter establishes the minimum requirements and standards for acquiring and managing digital certificates. It applies to all District and Central Office units within the FDOT. It establishes: AARF as the means to acquiring a digital certificate at FDOT, how digital certificate vendors are approved, installation and removal of digital certificates.

Sections include:

- 21.1.1 Procuring Digital Certificates
- 21.1.2 Approved Digital Certificate Vendors
- 21.1.3 Digital Certificate Accountability
- 21.2 Implementing Digital Certificates
- 21.2.1 Digital Certificate Security Assessments
- 21.3.1 Installation of Digital Certificates
- 21.3.2 Removal of Digital Certificates

CHAPTER 23 - Security and Use of Digital Certificates

This chapter establishes the requirements for the security and use of digital certificates within the Department's information technology infrastructure.

Sections include:

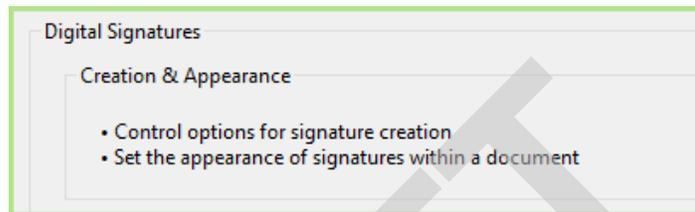
- 23.1 Use of Digital Certificates
- 23.2.1 Centralized Procurement of Digital Certificates

2 DOCUMENT SIGNING

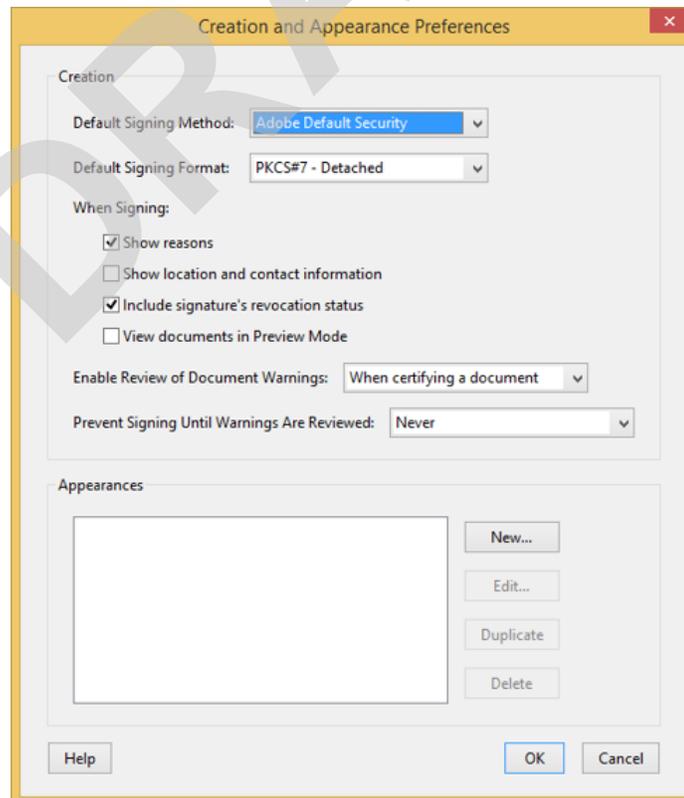
THE APPEARANCE

The digital signature appearance is a visible symbol and / or text that appears on an electronically produced document.

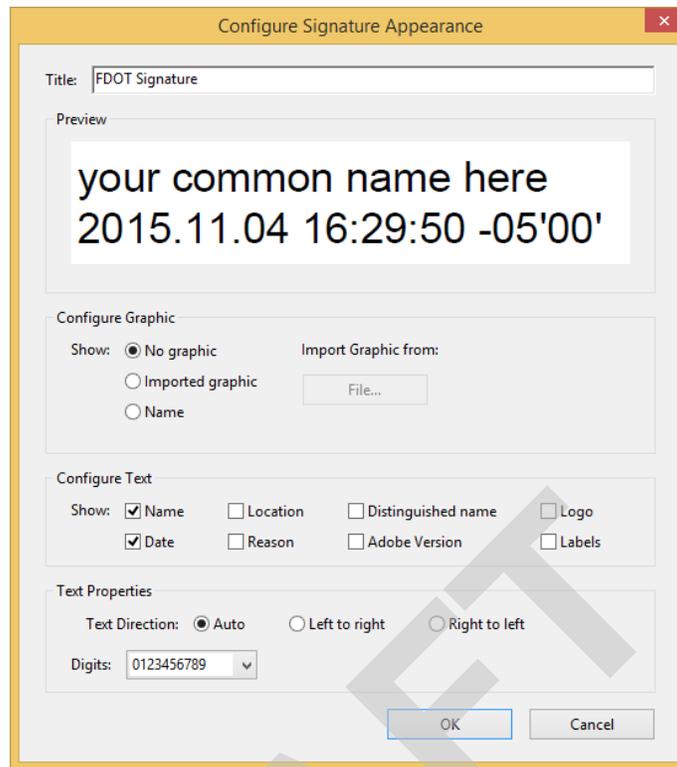
ADOBE



1. From the menu click **Edit > Preferences** or press **CNTL + K**.
2. From the Preferences dialog select **Signatures**.
3. At the Signatures dialog there should be a section Creation & Appearance as seen on the left. From this dialog click the More button. This will bring up the following dialog.



- Click **New** and the Configure Signature Appearance dialog will open.

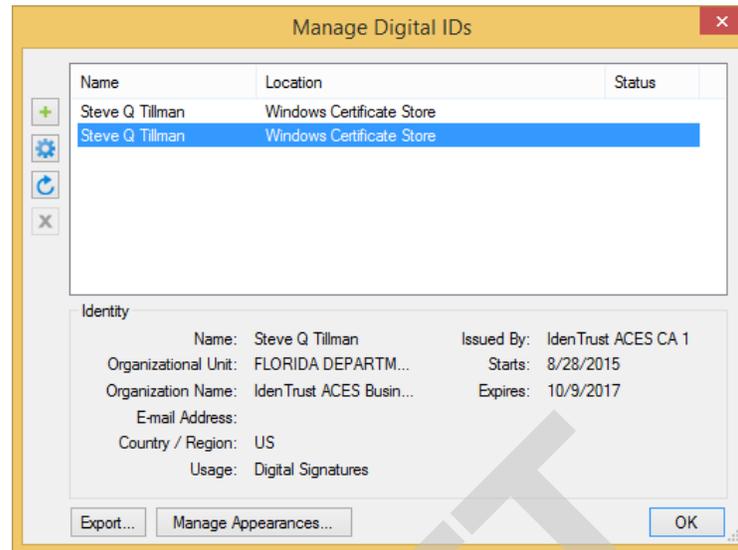


- Typical FDOT Adobe appearance.

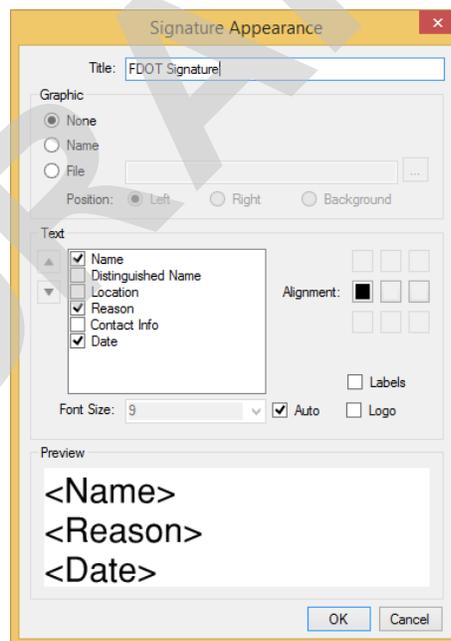


BLUEBEAM

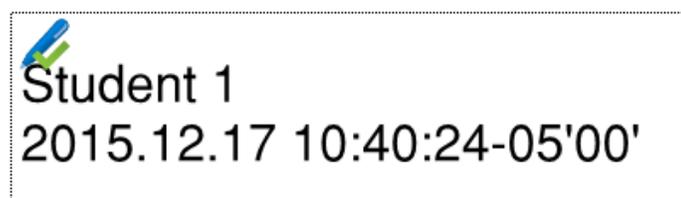
1. From the menu click **Document > Signatures > Digital ID's**.



2. Select a valid **Digital ID**.
3. Click the **Manage Appearances** button at the bottom. The **Signature Appearance** dialog displays.



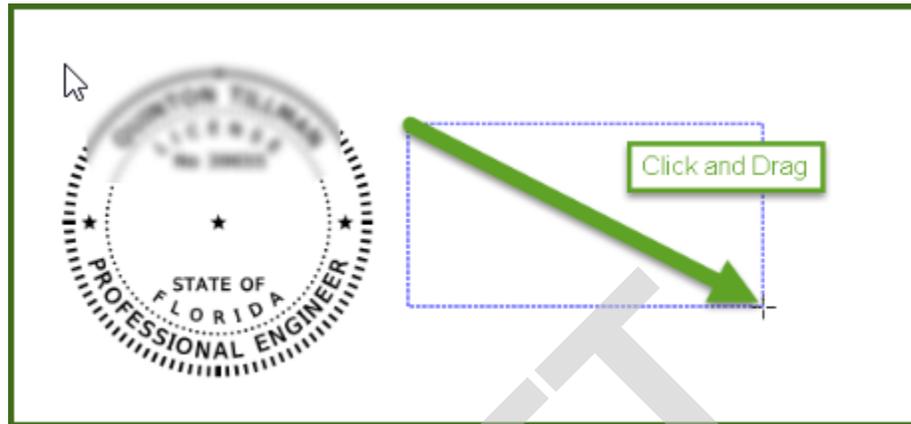
4. Typical FDOT BlueBeam appearance.



SIGNING A DOCUMENT

CLICK AND DRAG – THE QUICK AND DIRTY METHOD

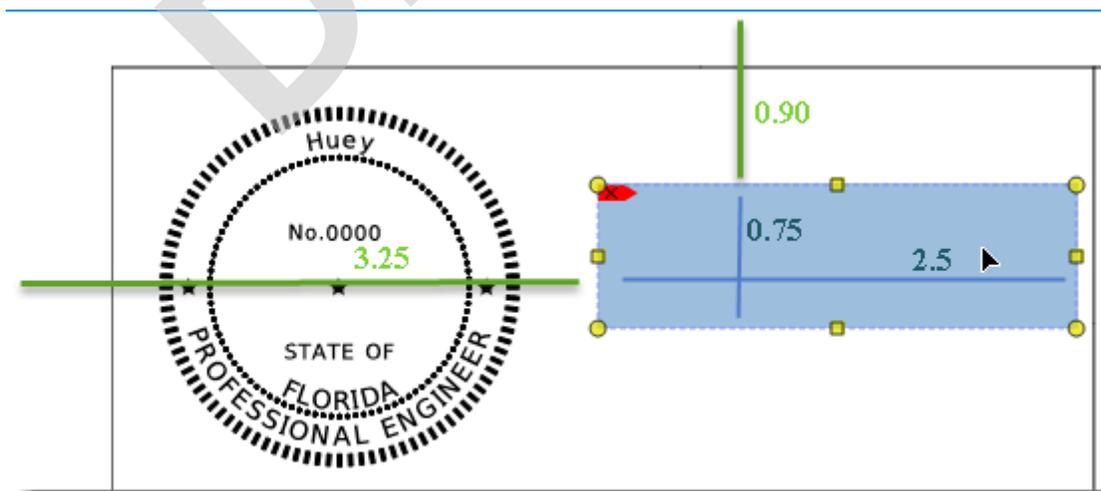
After the digital certificate has been installed and trusted by the signature application, the quickest and easiest method to sign a document is to click “Sign” from the menu and then click and drag a rectangle on the document where you want the signature placed. This creates a digital signature appearance.



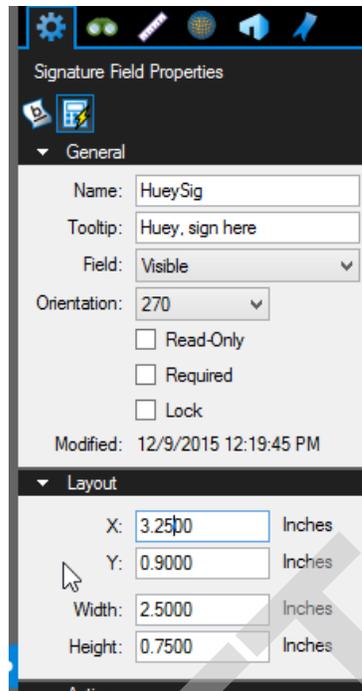
If the electronically produced document contains multiple pages or sheets, the digital signature appearance is placed only once on a document. The digital signature applies to the entire file; all sheets are signed. If any of the pages or sheets in the document are altered the digital signature is invalidated. In the case where there are multiple signatories or the single signatory does not intend to sign the entire document, qualifying language is used to limit the scope of the signature. On plan sets this is done with qualifying language and an index of the specific sheets the signatory intends to sign, located in immediate proximity to the digital appearance.

USING SIGNATURE BLOCKS

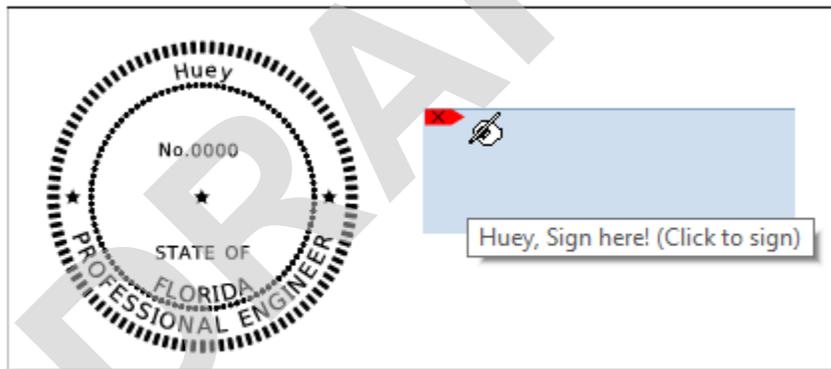
PDF documents can have a number of different types of form fields. There are text fields, radio buttons, check boxes and more. One type of field is a Digital Signature Field. These can be placed on the document prior to anyone signing. This gives more control over placement and size.



The signature fields can have names and tool tip that activate on mouse roll-over.



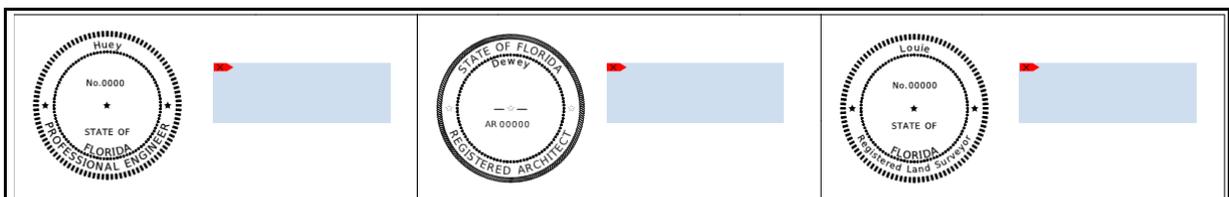
Once the document has all of the form fields in place, all the signatory needs to do is click the box and sign.



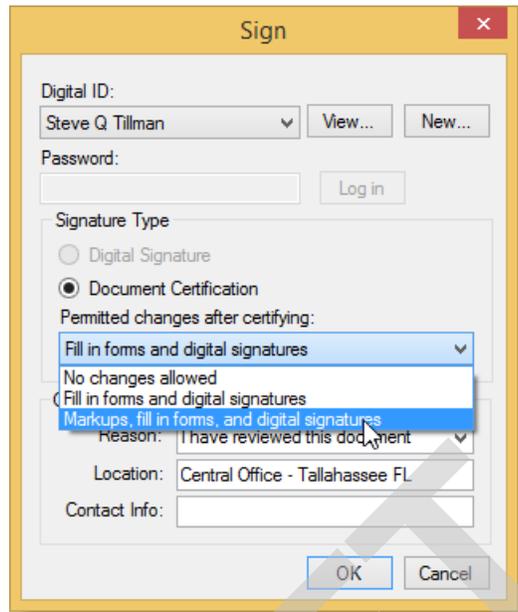
CERTIFYING THE DOCUMENT

By certifying a document, one can prevent unauthorized signatures and form changes. Certifying can specify what changes, if any are allowed to the document after it has been signed.

First the document is created as a multi-sheet PDF. Then use the form field editor to create the signature fields / blocks.



The illustration above shows three unsigned signature fields. These are as yet unsigned. Once the document is certified no more fields can be added to the document.



In fact, the only changes that can be made are signing the blank signature fields and placing mark-ups without invalidating the certificate. Mark-ups allow users to highlight, draw figures on the document, place stamps and etcetera. Basically any of the tools on the mark-up ribbon bar can be used without disturbing the certified document if mark-ups have been allowed by the certificate. This can be useful for subsequent users of the document.

SIGNING AND LINKING MULTIPLE DOCUMENTS

To be Determined

FLORIDA ADMINISTRATIVE CODE REGARDING DIGITAL SIGNATURE

The Florida Administrative Code (F.A.C.) has undergone a significant reorganization and rewrite. The new section 65G15-23 titled **SEALS** is effective as of November 3, 2015. The new section is organized as follows:

- **61G15-23.001** Signature, Date and Seal Shall Be Affixed (when, where and what to sign)
- **61G15-23.002** Seals Acceptable to the Board (what type of seal can be used)
- **61G15-23.003** Procedures for Physically Signing and Sealing Plans, Specifications, Reports or Other Documents (this relates to the paper signing process)
- **61G15-23.004** Procedures for Digitally Signing and Sealing Electronically Transmitted Plans, Specifications, Reports or Other Documents (this is the digital process using PKI)
- **61G15-23.005** Procedures for Electronically Signing and Sealing Electronically Transmitted Plans, Specifications, Reports or Other Documents (this is the old process with PEDDS)

Our focus for this training will be on section 61G15-23.004. In this section the Florida Board of Professional Engineers (FBPE) has addressed the use of digital signature. Nothing has changed with how the digital signature is utilized; what is new in the rule is how the FBPE has addressed the format of the appearance. There is now specific text that must accompany the digital signature. The following is extracted from the rule:

61G15-23.004 Procedures for Digitally Signing and Sealing Electronically Transmitted Plans, Specifications, Reports or Other Documents.

(1) Engineering plans, specifications, reports or other documents which must be signed, dated and sealed in accordance with the provisions of Section 471.025, F.S., and Rule 61G15-23.001, F.A.C. may be signed digitally as provided herein by the professional engineer in responsible charge. As used herein, the terms "certification authority," and "digital signature" shall have the meanings ascribed to them in Sections 668.003(2), (3) and (4), F.S.

(2) A professional engineer utilizing a digital signature to electronically sign and seal engineering plans, specifications, reports or other documents 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; and,

(d) Linked to a document in such a manner that the digital signature and correspondingly the document is invalidated if any data in the document is changed.

(3) The affixing of a digital signature to engineering plans, specifications, reports or other documents as provided herein shall constitute the signing and sealing of such items.

(a) A digitally created seal as set forth in Rule 61G15-23.002, F.A.C. may be placed where it would appear if the item were being physically signed, dated and sealed.

(b) The date that the digital signature was placed into the document must appear on the document in accordance with subsection 61G15-23.001(5), F.A.C. and where it would appear if the item were being physically signed, dated and sealed.

(c) The engineering plans, specifications, reports or other documents being digitally signed and sealed shall include text to indicate the following and place it where an original signature would appear if the item were being physically signed, dated and sealed:

1. The same information required by subsection 61G15-23.002(2), F.A.C. if a digitally created seal is not use;

2. The item has been electronically signed and sealed using a Digital Signature; and,

3. Printed copies of the document are not considered signed and sealed and all signatures must be verified on any electronic copies.

(d) Formatting of seals and text similar to that depicted below may be used.

1. When a digitally created seal is used:



This item has been electronically signed and sealed by C. S. Hammatt, PE. On [DATE] using a Digital Signature.

Printed copies of this document are not considered signed and sealed and the signature must be verified on any electronic copies

2. When a digitally created seal is not used:

C. S. Hammatt, State of Florida, Professional Engineer, License No. X

This item has been electronically signed and sealed by C. S. Hammatt, PE. On [DATE] using a Digital Signature.

Printed copies of this document are not considered signed and sealed and the signature must be verified on any electronic copies

(e) When engineering plans, specifications, reports or other documents contain multiple sheets or pages, the licensee may apply a single digital signature per electronically transmitted item as set out in Rule 61G15-23.001, F.A.C. A digital signature applied to an item in electronic form shall have the same force and effect as signing all of the individual sheets or pages contained within that item unless otherwise limited as specified in subsection 61G15-30.003(3), F.A.C.

(f) In the case where multiple licensees sign and seal a single item, each licensee shall apply their digital signature and include qualifying language with those items required in paragraph (e) of this rule thoroughly describing what portions the licensee is taking responsibility for.

Rulemaking Authority 471.025(1), 471.033(2), 471.008 FS. Law Implemented 471.025, 471.033(1)(d), 668.006 FS. History-New 11-3-15.

The full text of the rule can be found on-line at the following address;

<https://www.flrules.org/gateway/ChapterHome.asp?Chapter=61G15-23>

3 FDOT DIGITAL PRODUCTION & DELIVERY

PROJECT PRODUCTION

Chapter 4 of the CADD Manual establishes the minimum requirements for production of FDOT CADD Projects in accordance with FDOT’s plans preparation procedures & practices. Chapter 4 establishes folder structure, file naming, print image file naming, and more. For more information on creating and producing projects, see the FDOT CADD Manual at:

[FDOT CADD Manual - CHAPTER 4 - CADD PRODUCTION PROCEDURES](#)

Note Section 4.12.5 addresses the Professional of Record Note. This section is out of date due to changes in administrative rule. Always check with you board of professional regulation for the correct reference to F.A.C. rule number.

PROJECT CREATION

To create a project use the Create Project application. This application creates a folder structure that complies with FDOT standards. Information gathered by Create Project is used to populate title blocks on plan sheets and by many other processes. The folder structure and file names are still the same; nothing has changed with regard to file names and structure with one exception, the Specs Only project.

1. Launch Create Project:

Create FDOT Project (Version 5.1.11.12)

Project Type
This application can create both AutoCAD and Micro-Station FDOT projects. By selecting the type of project you wish to create, the application can setup the appropriate directory structure and the other required components specific the type of project selected.

FDOT AutoCAD Civil 3D Project **FDOT MicroStation Project**

Parent Container Directory
The Parent Container Directory is the root directory that holds your new and existing projects. Once you click the "Create Project" button, your new project directory and its corresponding sub-directory structure will be created under this parent container directory. (Example: C:\e\projects)

Parent Directory: C:\Projects\Civil3D\

Financial Project Information
The financial project information is used to generate the Financial Project Identifier (FPID). New projects will always be created under the Parent Container Directory in a new directory named from the concatenation of the financial project information fields.

Item: 219843 **Segment:** 1 **Phase Group:** 5 **Phase Type:** 2 **Sequence:** 01

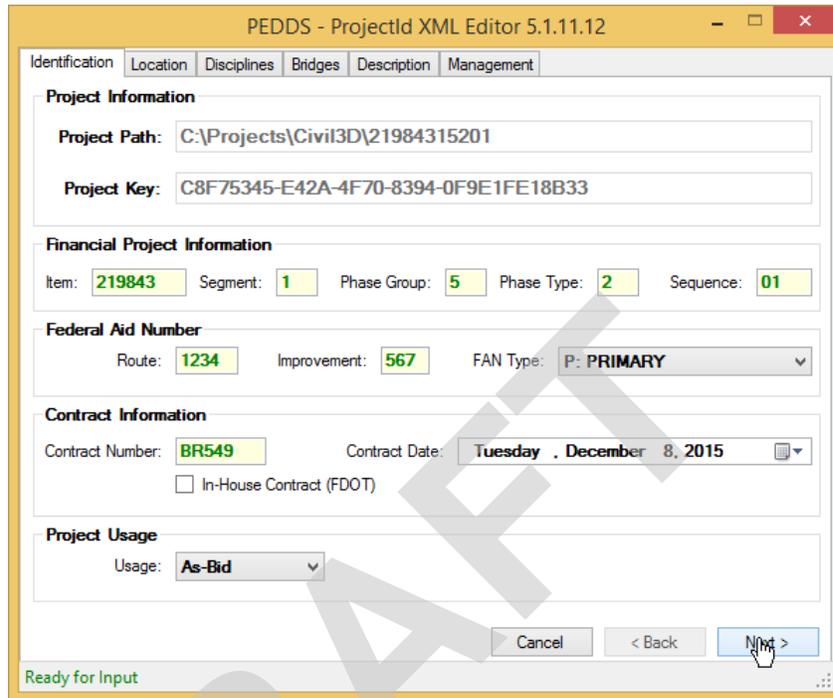
Contract Information
Contract Number: BR549 **Contract Date:** Tuesday, December 8, 2015
 In-House Contract (FDOT)

Project Description
General Description
This project is a simulation of a 3D Design with Digital Delivery. Some of the data in this project may have been taken from actual FDOT projects. However, no portion of this project may be construed to represent an actual design.

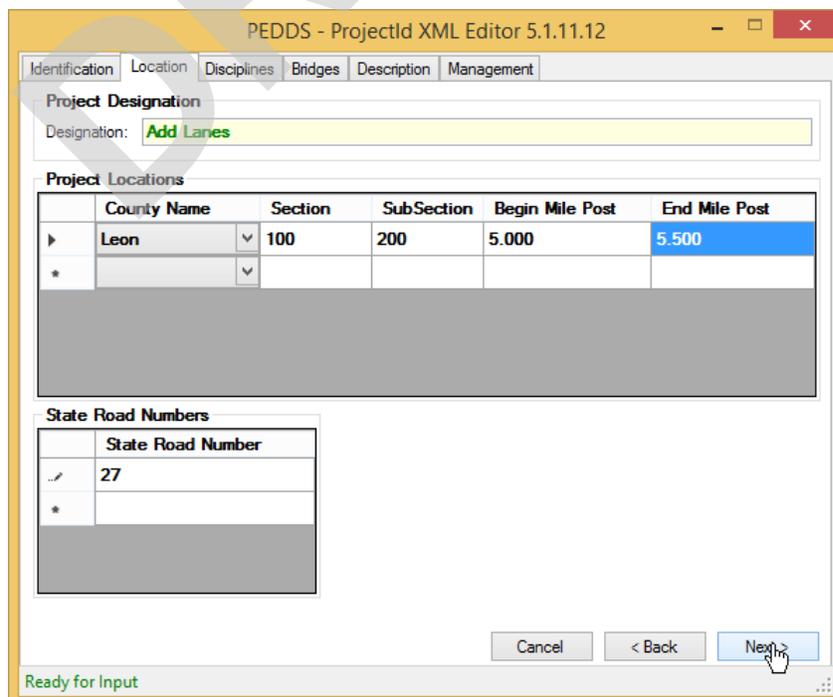
Cancel Finish

Required Fields

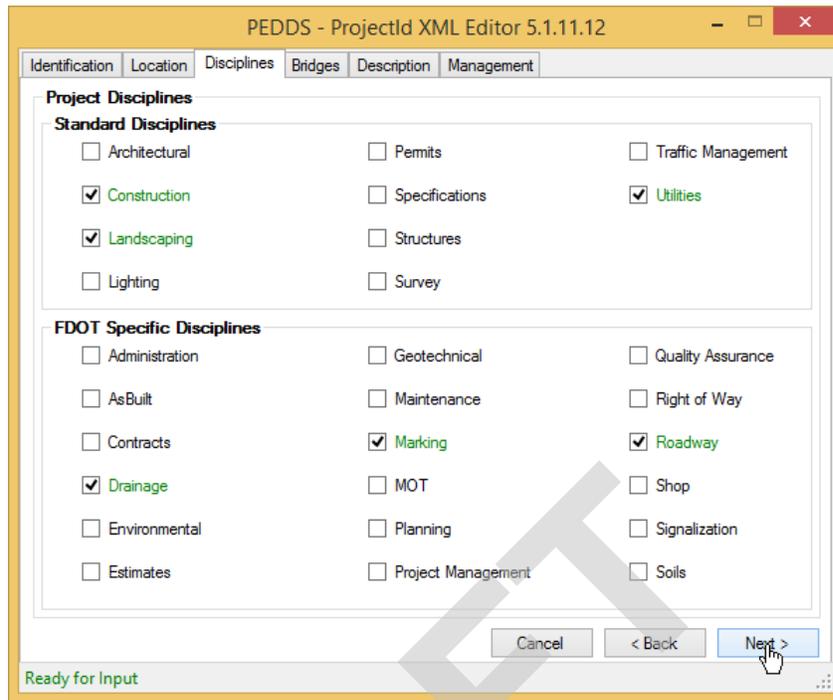
2. This application will create a project that is either AutoCAD or MicroStation specific. Ensure that your CADD environment is not up and running when you launch this. Fill in the required fields. Notice that they turn green when populated. Click **Finish**. You will see a confirmation screen, click **OK**.
3. Next, if all goes smoothly, the Project Id XML Editor will open. It has six specific data categories that define the project: *Identification*, *Location*, *Disciplines*, *Bridges*, *Description*, and *Management*. In the *Identification* tab, the information will fill-in from the initial project create. Click **Next**.



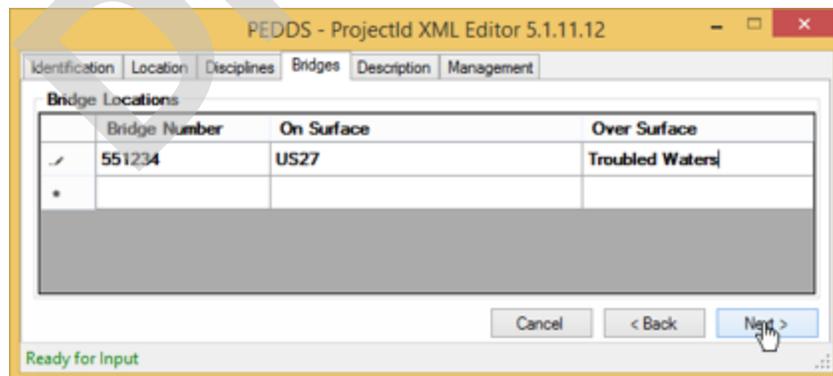
4. In the *Location* tab, input the required information. Click **Next**.



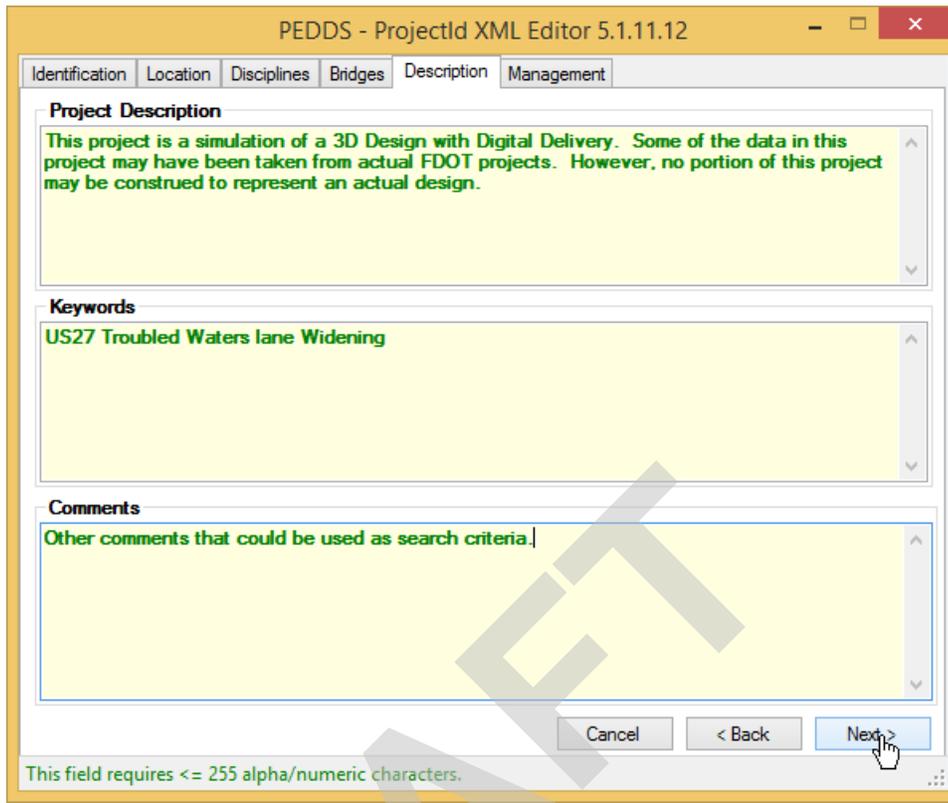
5. In the Discipline tab, select as indicated below. Click **Next**.



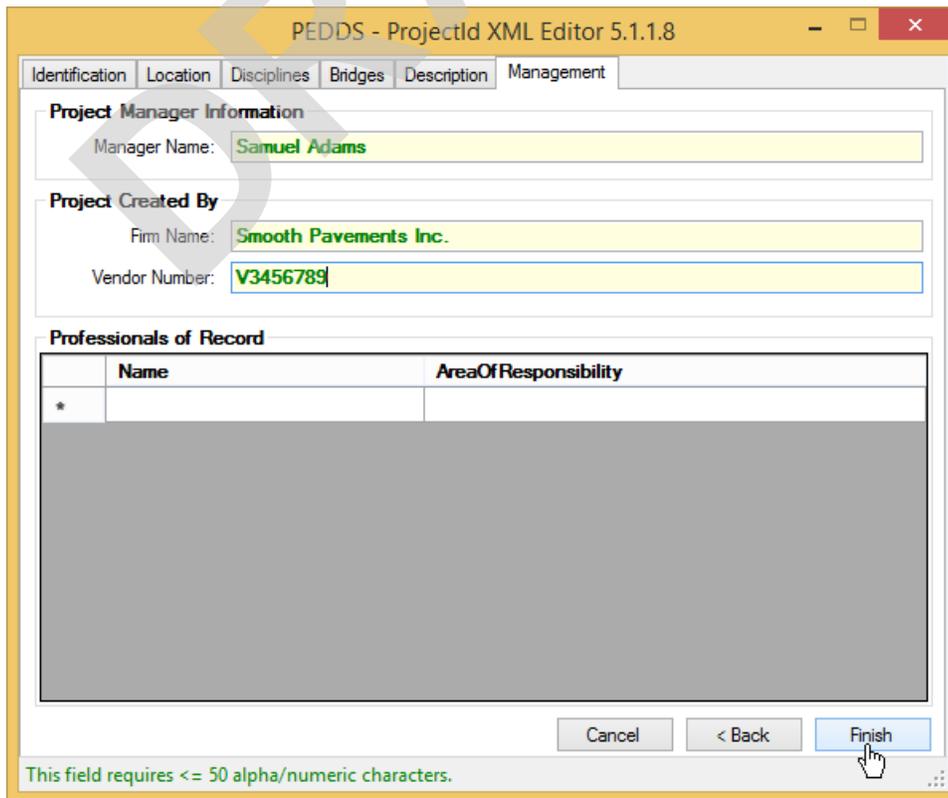
6. The *Bridges* tab is the dialog of much confusion! If there are bridges on the project, input the bridge number. The next two fields, *On Surface* and *Over Surface*, are used as follows:
 - a. *On Surface* – the travel way that is supported by the surface of the bridge. This will be the name of the roadway, railway, pedestrian overpass or critter crossing supported on the surface of the bridge.
 - b. *Over Surface* – the travel way that the bridge is passing over. This also will be the name of the roadway, railway or waterway.



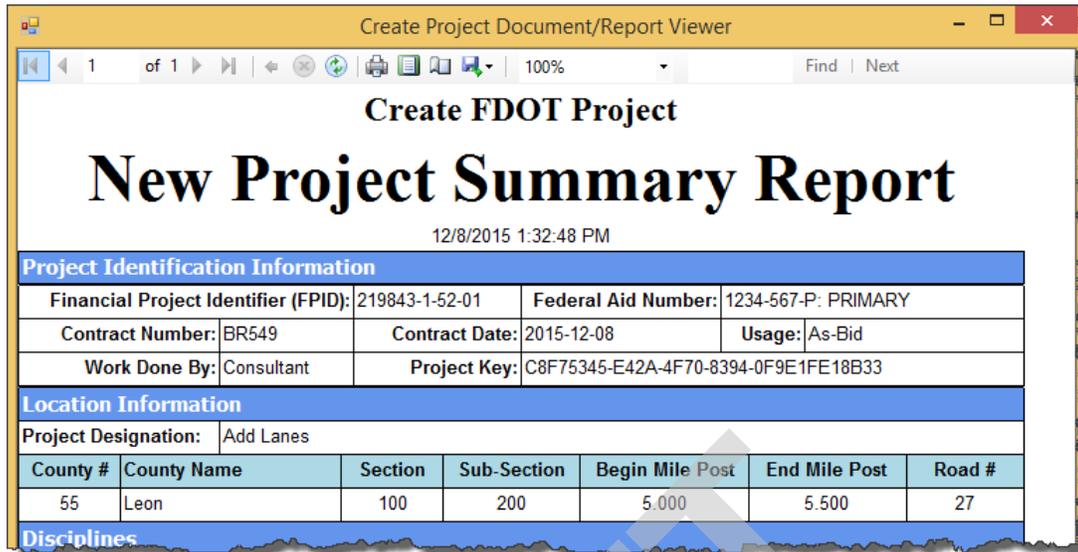
- In the *Description* tab, the information that can be used as search criteria later.



- And finally the Management tab as follows and click **Finish**.



9. You should see a confirmation screen. Click **OK**. At last you will see a report indicating that the project was successfully completed. This takes a minute to complete.



PROJECT DELIVERY

Chapter 5 of the CADD Manual provides information on FDOT’s delivery process:

[FDOT CADD Manual - CHAPTER 5 - DELIVERY PROCEDURE](#)

5.5 RECEIPT AND ACCEPTANCE OF ELECTRONIC DATA

The Project Manager is responsible for ensuring that the terms of the scope of services of a project have been met, including the assurance that the Department’s Quality Control requirements were fulfilled during production of the electronic data.

- Receipt of Data: The Project Manager must receive electronic data under a letter of transmittal.
- Authentication: Upon receipt of the delivery media, the Department will validate all Digitally Signed files.
- Acceptance: The Project Manager ensures that the delivery is checked for completeness and meets the terms, conditions and requirements outlined herein. Once the delivery has been determined to be compliant, a record of acceptance must be made

5.8 DIGITAL DELIVERY

Digital Signature is defined in Florida Statutes 668.003 and uses a Digital Signature to secure files. Digital Signature is a “paperless” process that relies upon the intrinsic ability of the files themselves to encode cryptographic security features using a Digital Certificate issued to the Professional of Record.

The Digital Delivery comprises two parts:

- Part that represents the work product of design in the full project directory structure
- Part extracted from the full project directory structure that will be provided to contractors as defined in 5.8.1 below.

5.8.1 Production Deliverable Files

- An archive containing CAD data and other project files useful to construction contractor – CADD.ZIP
- A PDF representation of the plans set – PLANS.PDF
- A PDF containing the specifications – SPECS.PDF

PLAN SETS BY COMPONENT

When and how to divide plan sets by depends on the size and complexity of the project. How the project will be divided must be determined by district production prior to delivery. Generally, when there are multiple professionals of record per component or when the size of the resulting PDF is so large that it is incompatible with available computer equipment and software. Division by sheet range must only be done in extreme cases where the size

The following convention will be used when naming the Bid Set Files:

<Fpid> - <FileDescription> - <PlansComponentCode> - <ComponentDescription> - <OptionalSheetRange> - <OptionalDescription>.PDF

Example: 01234567890-PLANS-01-ROADWAY-023-200-DRAINAGE-STRUCTURES.PDF

- **FPID** - The files delivered for the Bid Set will always begin with the eleven digit Financial Project Identification (FPID) number followed by a dash as a separator. (Required)
- **File Description** – One of three terms (PLANS, SPECS, CADD) describing the contents of the file is added. (Required)

The PLANS portion of the delivery will often be made up of multiple PDF files. When there are multiple files making up the delivery for a particular type of data (PLANS, SPECS, and CADD), additional attributes will need to be included in the name.

- **PlansComponentCode** – Next a two digit code representing the order components are inserted into the plans set is added followed by a dash as a separator. (Required if divided by plans component)
- **ComponentDescription** - A text string describing the component is added followed by a dash as a separator. (Required if divided by plans component)

EARLY WORK

Some parts of a project are done prior to the design phase. These are called **early work**. Examples of early work include Right of Way surveys, establishment of Project Network Control (PNC), Geological surveys (Core Borings) and Verification of Underground Utilities. Portions (certain early works sheets) of a plan set that are delivered early in the project development cycle may be digitally signed at the time of sheet development. In so doing, the professional of record will sign said early works sheets only once when those sheets were completed, unless subsequent changes are made to the sheets.

An example might be the Project Network Control (PNC) sheets; a Professional Surveyor & Mapper (PSM) may sign the PNC sheets once they are prepared, and deliver those sheets as a completed document. Other examples might include Soil Core Borings and Verified Utilities, which also happen early in the design and plans preparation process.

When a Plans Component PDF must be further subdivided and include early works as described above, the following table shows file name examples that may be used:

- fpid-PLANS-01-ROADWAY-PNC.PDF
- fpid-PLANS-01-ROADWAY-COREBORINGS.PDF
- fpid-PLANS-01-ROADWAY-VERIFIEDUTILITIES.PDF

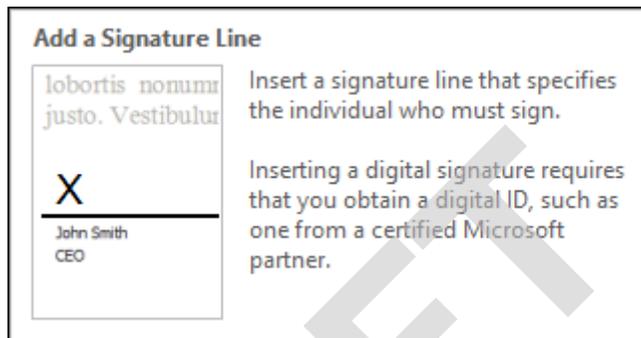
The distinction shows the intended Plans Component PDF that the early works sheets are intended to belong to, along with a keyword (PNC, COREBORINGS, etcetera) describing the content of the PDF delivered. In no case should this be construed to imply the delivery of random sheets signed by a single Signatory, or a collection of non-consecutive sheets in a single file by one Signatory. The plans producers must consider the user of the plans when making decisions about whether and how to subdivide a plans set. Subdivision should balance the needs of the plans producers and plans users. All sheets of a Plans Component PDF, or even the early works sheets described above, will be in consecutive sheet order and suitable for inclusion into the overall set.

4 Other Types of Documents

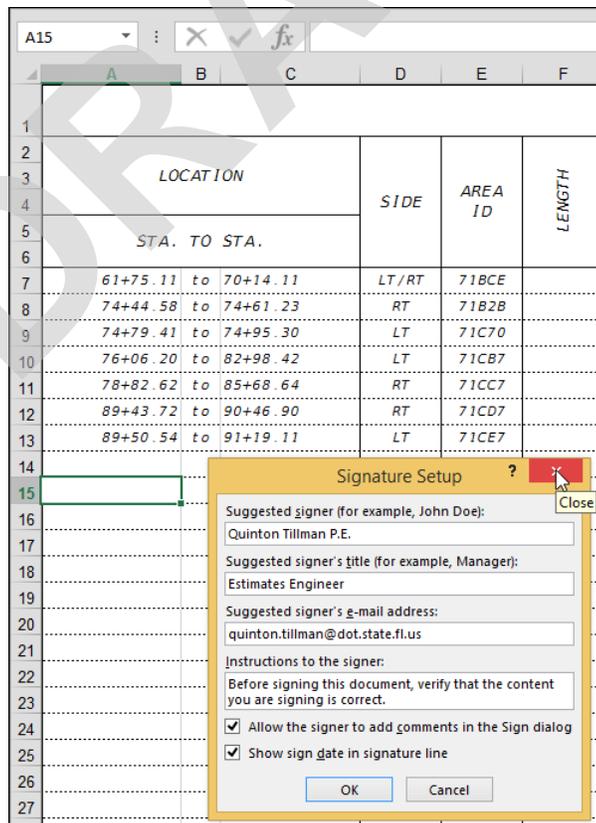
MICROSOFT OFFICE SUITE

To apply a digital signature to an Excel spreadsheet.

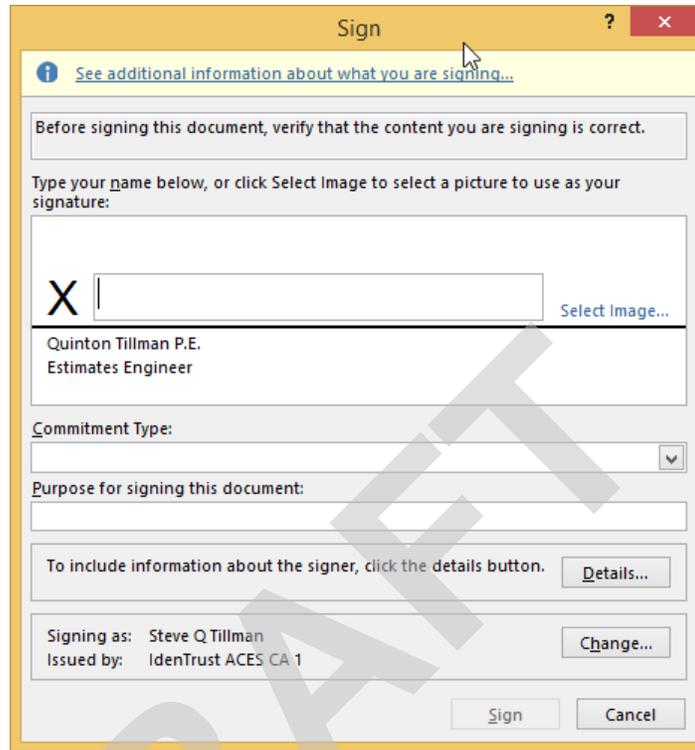
1. Open a spreadsheet and select a cell where you would like the signature block (digital signature appearance) to be placed. This will be the upper left corner of the block. From the menu select **Insert**.



2. From the *Insert* ribbon bar select **Text > Signature Line**. The signature line just creates a place on the spreadsheet to put a signature. Click *Signature Line* and the following dialog will open:



3. Fill in the information requested. Click **Ok** and the *Signature Line* is now placed on the spread sheet along with the name and title of the individual who is supposed to sign the document. Still no digital signature; we're not there yet.
4. The next step requires a digital certificate. Right-click on the *Signature Line* and select **Sign....** The following dialog will display:



5. Either type *your name* or select *an image*. Fill in other information as requested. Finally, ensure that the proper certificate has been selected. Click **Sign**. A windows security dialog will appear. Type the certificate signing password and click **Ok**. The document is now signed.



The document is now signed and protected. All of the functions on the ribbon bar that alter the spread sheet are now disabled. This does not, however, prevent the document from being altered.

DATA TYPES TO BE DELIVERED

Chapter 5 of the CADD Manual provides information on FDOT's types of data to be delivered:

5.10.2 Engineering Data

In addition to the delivery of the files produced during the course of development, the Department requires the inclusion of certain Engineering Data files for critical geometrics in the design. These can include the alignments, profiles, cross sections, and surfaces. Critical roadway geometric items, such as the centerlines and profiles of the proposed mainline, side streets, special ditches, and utilities, must be included.

5.10.2.1 *Delivery Standards for Engineering Data*

The required formats for Engineering Data files for a project as part of the Delivery includes LandXML, which covers basic geometry element types, and is readable by the Department's software systems, from both Bentley and Autodesk. In addition, LandXML may be consumed by many software used by the highway construction industry including AGTEK, Trimble, Carlson, and others.

The LandXML format defines data exchange format for basic roadway geometrics including:

- Point data
- Profiles
- Curve data
- Pipe Networks
- Spiral data
- Terrain Model Surfaces
- Alignments (with station equations)
- Survey Data.
- Cross Sections (surface and design sections)

LandXML is widely supported by many civil engineering software. Read more about LandXML at:

<http://www.LandXML.org>

XML SIGNING

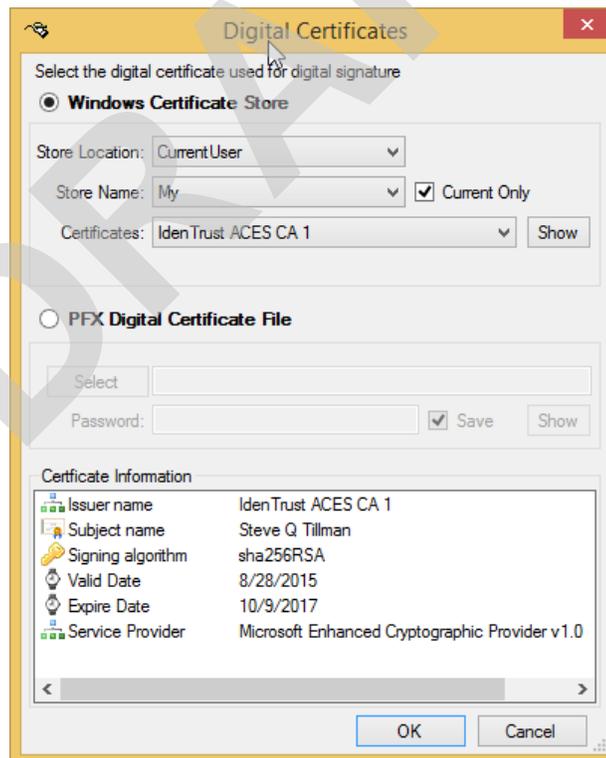
```

<Alignments>
  <Alignment name="AL1" length="16966.9819079761" staStart="69733.26"
    desc="S.R. #10 FROM WEST OF DEMPSEY MAYO ROAD TO S.R. #8 (INTERSTATE 10)">
    <CoordGeom desc="BL">
      <Line length="400.000000260832" dir="67.2430555841454">
        <Start>533248.004677 2059335.38902 151.762</Start>
        <End>533402.73377 2059704.250658 151.762</End>
      </Line>
      <Line length="449.999999746911" dir="67.2430555031943">
        <Start>533402.73377 2059704.250658 151.762</Start>
        <End>533576.804 2060119.22 151.762</End>
      </Line>
      <Line length="4880.871814421" dir="67.2812036604856">
        <Start>533576.804 2060119.22 151.762</Start>
        <End>535461.839 2064621.392 184.229</End>
      </Line>
      <Line length="7396.83575305686" dir="67.2244923985917">
        <Start>535461.839 2064621.392 184.229</Start>
        <End>538325.313 2071441.487 133.276</End>
      </Line>
      <Line length="3839.27434049047" dir="67.2282241455335">
        <Start>538325.313 2071441.487 133.276</Start>
        <End>539811.348 2074981.505 67.412</End>
      </Line>
    </CoordGeom>
  </Alignment>
</Alignments>

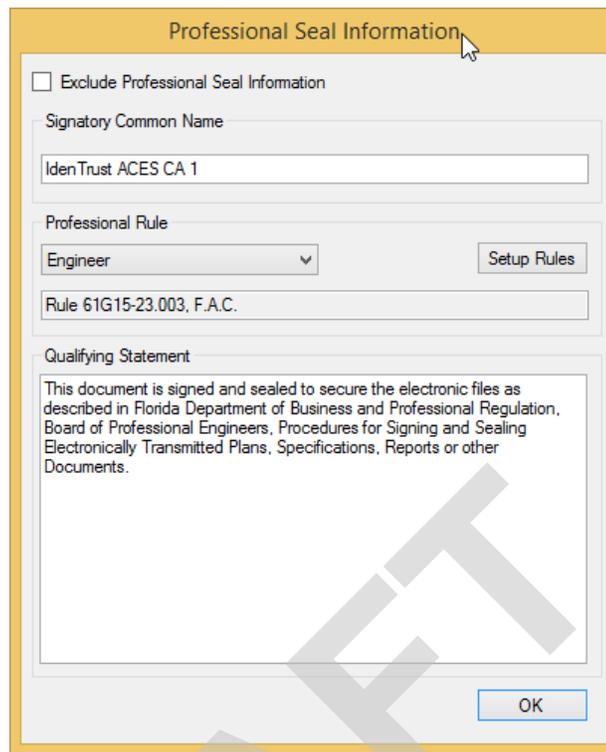
```

A digital certificate can be applied to XML data using the FDOT XML Signing application.

1. First select a certificate for signing.



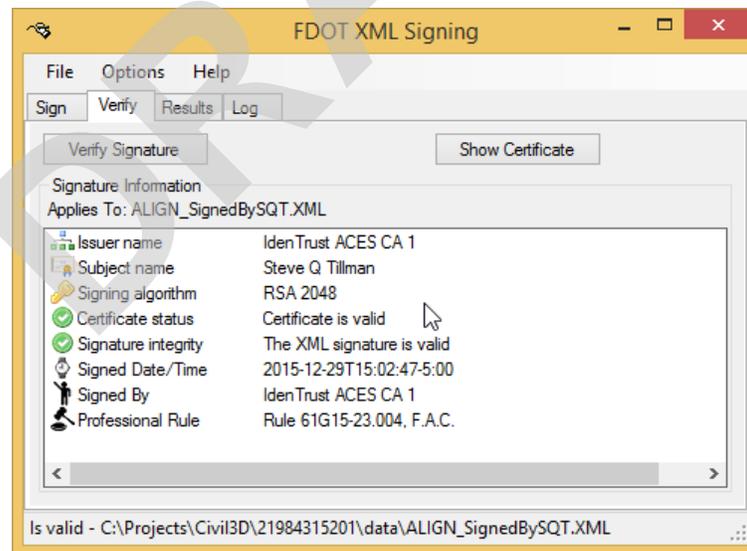
2. Make sure you have the correct one and check *Professional Rule* to ensure correct.



The image shows a dialog box titled "Professional Seal Information". It contains the following fields and controls:

- Exclude Professional Seal Information
- Signatory Common Name: IdenTrust ACES CA 1
- Professional Rule: Engineer (dropdown menu) with a "Setup Rules" button next to it.
- Rule 61G15-23.003, F.A.C. (text field)
- Qualifying Statement: This document is signed and sealed to secure the electronic files as described in Florida Department of Business and Professional Regulation, Board of Professional Engineers, Procedures for Signing and Sealing Electronically Transmitted Plans, Specifications, Reports or other Documents.
- OK button

3. Next Click **Apply Signature**, select *file*, enter certificate *Signing Password* and sign.



The image shows the "FDOT XML Signing" application window. It has a menu bar with "File", "Options", and "Help". Below the menu bar are buttons for "Sign", "Verify", "Results", and "Log". There are also buttons for "Verify Signature" and "Show Certificate".

The "Signature Information" section displays the following details:

Signature Information	
Applies To: ALIGN_SignedBySQT.XML	
Issuer name	IdenTrust ACES CA 1
Subject name	Steve Q Tillman
Signing algorithm	RSA 2048
Certificate status	Certificate is valid
Signature integrity	The XML signature is valid
Signed Date/Time	2015-12-29T15:02:47-5:00
Signed By	IdenTrust ACES CA 1
Professional Rule	Rule 61G15-23.004, F.A.C.

At the bottom of the window, it says: "Is valid - C:\Projects\Civil3D\21984315201\data\ALIGN_SignedBySQT.XML"