So, what is a digital delivery and how does it differ from what we have been doing for the past decade at FDOT?

I am Quinton Tillman from the FDOT - ECSO and I would like to answer that question examining three aspects of our current delivery methods. Teresa and Jamie have done an excellent job on presenting the efficiencies gained in the districts with Digital Delivery and how the process has been implemented.

As we move forward with this process, let's look at the following.

Consistent
Predictable
Repeatable

Progress

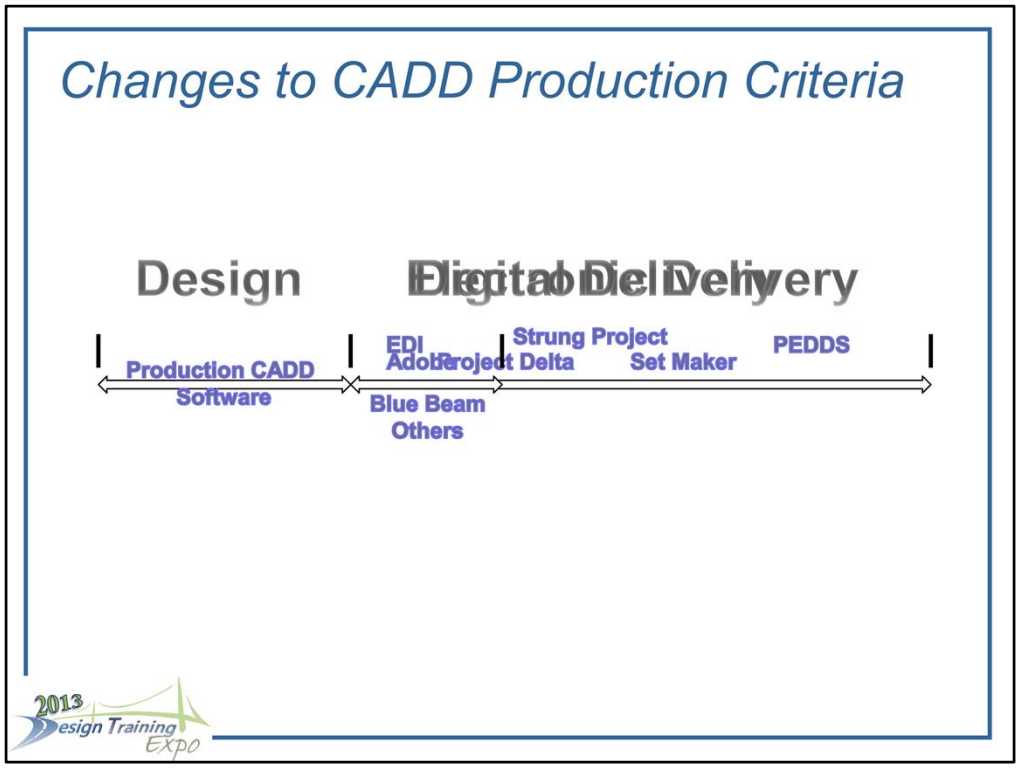
Bold
Innovative
Inspirational

Potential
Possible
Practical

2013 Design Training Expo

From Paper to "Electronic" to "Digital"

- Changes to the CADD Policy
  - ✓ FDOT CADD Manual
  - ✓ CADD Production Criteria Handbook (CPCH)
- "Electronic" vs. "Digital"
- Why change?



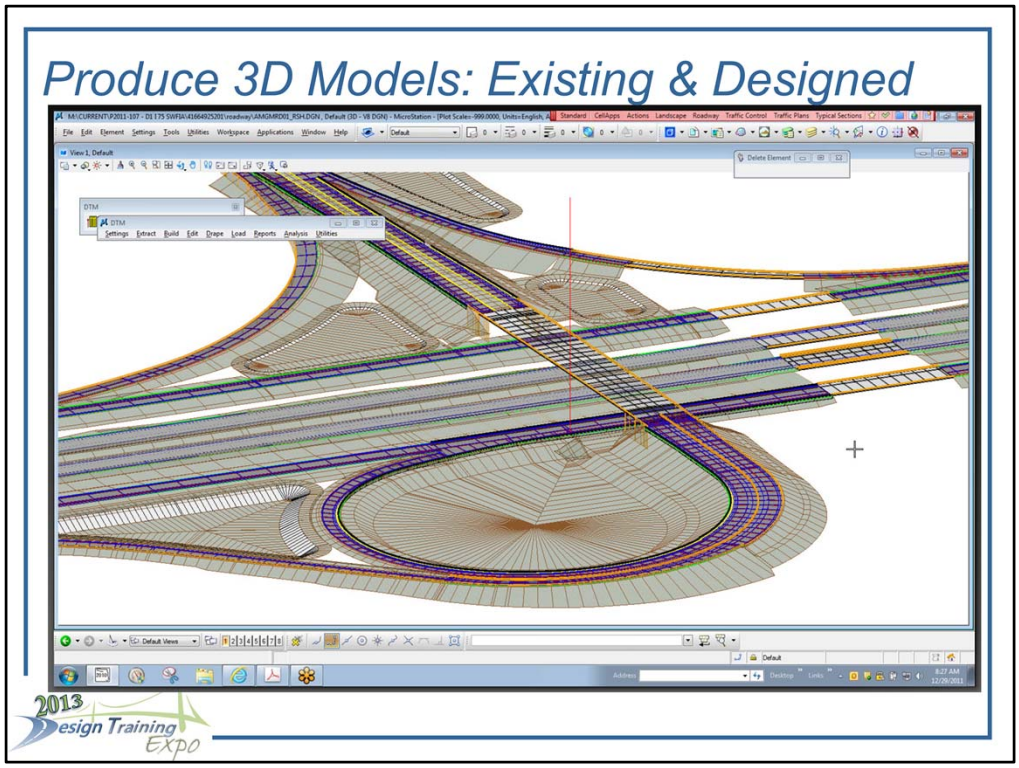
Pain points

Sheet navigator may be used to manage

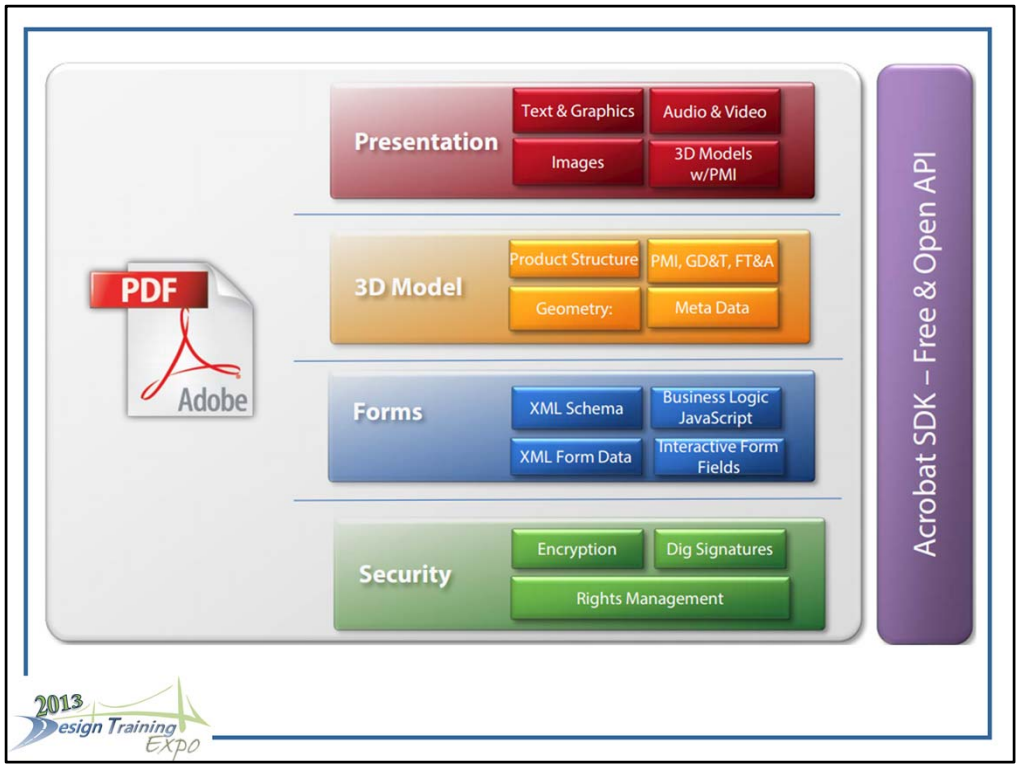
What is "Digital Delivery"?

- A contemporary method of ~~Electronic~~ **Digital Delivery** that relies more upon the **PDF** of the plans / specs being created, with fidelity. PDF has future potential and 3D data exchange possibilities.
- The production of a CADD Index is no longer required (nor the associated programs, files or reports), so no need for the tools EDI, SetMaker, ProjectDelta, StrungProject, etc. for Digital Delivery.
- Digital Signature (as opposed to PEDDS' implementation of Electronic Signature) used as the principal means to secure the plans and specifications PDF files.
- CADD files & "Engineering Data" compiled into a ZIP file for the contractor pre-bid, and more emphasis on **3D models**

2013 Design Training Expo



A major emphasis moving forward is the employment of the 3D Design techniques to model the facility to encourage the deployment of AMG in construction. Models can be produced as: 3D MicroStation files, AutoCAD Files (DWG or DXF), or LandXML files. We need files of the pre-construction Existing Terrain Surface, and the final Proposed Design Surface.


PDF
Adobe
Presentation
Text & Graphics
Audio & Video
Images
3D Models w/PMI
3D Model
Product Structure
PMI, GD&T, FT&A
Geometry:
Meta Data
Forms
XML Schema
Business Logic JavaScript
XML Form Data
Interactive Form Fields
Security
Encryption
Dig Signatures
Rights Management
Acrobat SDK – Free & Open API
2013 Design Training Expo

3D PDF is an interesting option

- Access
  - ✓ through Acrobat Reader
- Multi-type
  - ✓ 3D, 2D, image, text, audio, video, enterprise data
- Fit for purpose
  - ✓ Scripting support, templates, forms, portfolios
- Infrastructure
  - ✓ existing systems and resources already support PDF
- Neutrality
  - ✓ Investment protection

2013 Design Training Expo

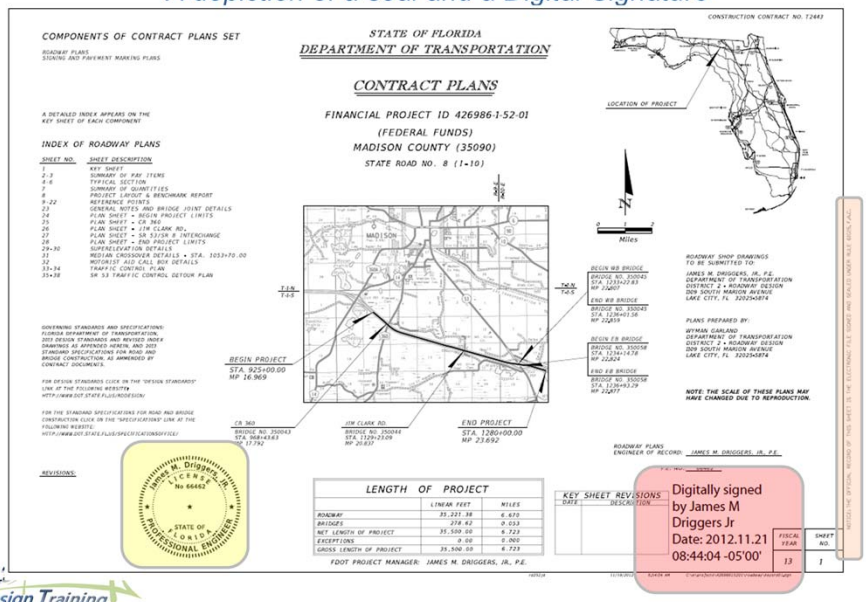
So then, What did not change?

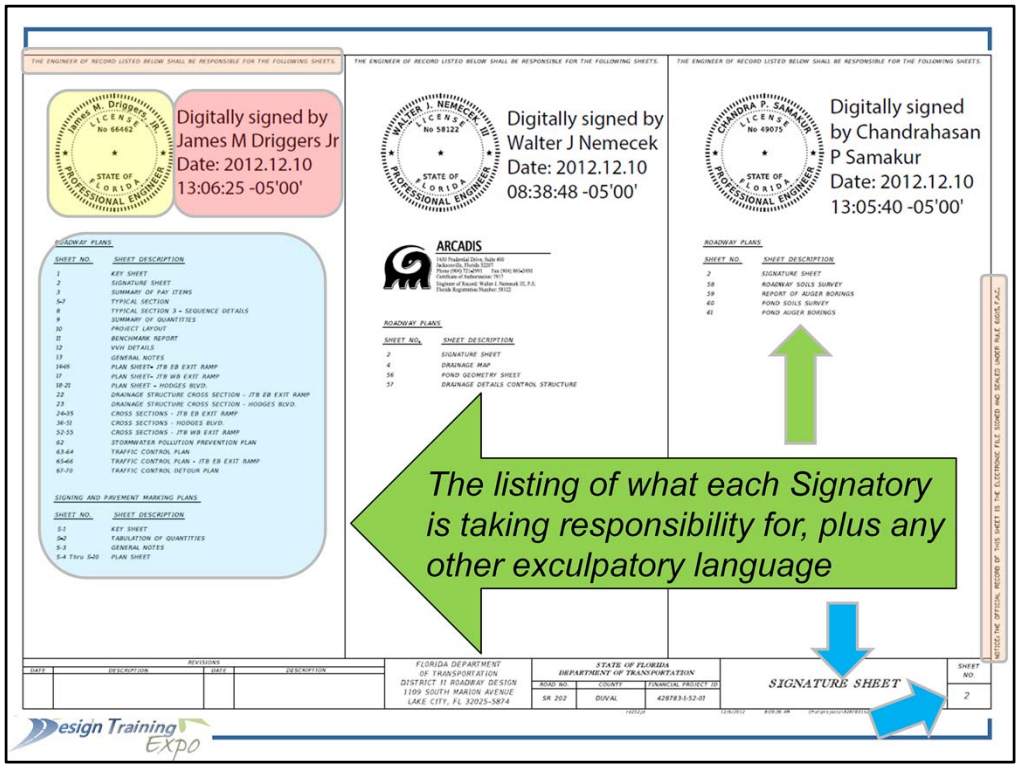
- You will still make a “Project CD” delivery of your work:
  - ✓ You still work in a prescriptive project directory structure, follow CADD file naming and content standards, and follow CADD symbology standards
  - ✓ You still perform CADD QC on your CADD files and they still need to be compliant
- You still make a PDF of the Plans (but the name changes slightly - for distinction between Classical Electronic and Delivery and Digital Delivery)
- You still make PDFs of the Specs
- You still secure your plans and specs, just by a different means (certificate based Digital Signature)

2013 Design Training Expo

Plans Signed with a "Digital Signature"

A depiction of a seal and a Digital Signature




THE ENGINEER OF RECORD LISTED BELOW SHALL BE RESPONSIBLE FOR THE FOLLOWING SHEETS.
James M. Driggers, Jr.
LICENSE
No 66462
STATE OF FLORIDA
PROFESSIONAL ENGINEER
Digitally signed by James M Driggers Jr
Date: 2012.12.10 13:06:25 -05'00'
ROADWAY PLANS
SHEET NO. SHEET DESCRIPTION
1 KEY SHEET
2 SIGNATURE SHEET
3 SUMMARY OF PAY ITEMS
5-7 TYPICAL SECTION
8 TYPICAL SECTION 3 - SEQUENCE DETAILS
9 SUMMARY OF QUANTITIES
10 PROJECT LAYOUT
11 BENCHMARK REPORT
12 VVH DETAILS
13 GENERAL NOTES
14-16 PLAN SHEET- ITB EB EXIT RAMP
17 PLAN SHEET- ITB WB EXIT RAMP
18-21 PLAN SHEET - HODGES BLVD.
22 DRAINAGE STRUCTURE CROSS SECTION - ITB EB EXIT RAMP
23 DRAINAGE STRUCTURE CROSS SECTION - HODGES BLVD.
24-35 CROSS SECTIONS - ITB EB EXIT RAMP
36-51 CROSS SECTIONS - HODGES BLVD.
52-55 CROSS SECTIONS - ITB WB EXIT RAMP
62 STORMWATER POLLUTION PREVENTION PLAN
63-64 TRAFFIC CONTROL PLAN
65-66 TRAFFIC CONTROL PLAN - ITB EB EXIT RAMP
67-70 TRAFFIC CONTROL DETOUR PLAN
SIGNING AND PAVEMENT MARKING PLANS
SHEET NO. SHEET DESCRIPTION
5-1 KEY SHEET
5-2 TABULATION OF QUANTITIES
5-3 GENERAL NOTES
5-4 Thru 5-40 PLAN SHEET
THE ENGINEER OF RECORD LISTED BELOW SHALL BE RESPONSIBLE FOR THE FOLLOWING SHEETS.
WALTER J. NEMECEK, III
LICENSE
No 58122
STATE OF FLORIDA
PROFESSIONAL ENGINEER
Digitally signed by Walter J Nemecek
Date: 2012.12.10 08:38:48 -05'00'
ARCADIS
ROADWAY PLANS
SHEET NO. SHEET DESCRIPTION
2 SIGNATURE SHEET
4 DRAINAGE MAP
56 POND GEOMETRY SHEET
57 DRAINAGE DETAILS CONTROL STRUCTURE
THE ENGINEER OF RECORD LISTED BELOW SHALL BE RESPONSIBLE FOR THE FOLLOWING SHEETS.
CHANDRA P. SAMAKUR
LICENSE
No 49075
STATE OF FLORIDA
PROFESSIONAL ENGINEER
Digitally signed by Chandrahasan P Samakur
Date: 2012.12.10 13:05:40 -05'00'
ROADWAY PLANS
SHEET NO. SHEET DESCRIPTION
2 SIGNATURE SHEET
38 ROADWAY SOILS SURVEY
39 REPORT OF AUGER BORINGS
40 POND SOILS SURVEY
41 POND AUGER BORINGS
The listing of what each Signatory is taking responsibility for, plus any other exculpatory language
NOTICE: THE OFFICIAL RECORD OF THIS SHEET IS THE ELECTRONIC FILE SIGNED AND SEALED UNDER RULE 61G15-F.A.C.
REVISIONS
DATE DESCRIPTION DATE DESCRIPTION
FLORIDA DEPARTMENT OF TRANSPORTATION
DISTRICT 11 ROADWAY DESIGN
1109 SOUTH MARION AVENUE
LAKE CITY, FL 32025-5874
STATE OF FLORIDA
DEPARTMENT OF TRANSPORTATION
ROAD NO. COUNTY FINANCIAL PROJECT ID
SR 202 DUVAL 428783-1-52-01
SIGNATURE SHEET
SHEET NO.
2
Design Training Expo

Changes to CADD Production Criteria

First Delivery

File Name	Contents
fpid#-CADD[-?].ZIP	Native CAD files and design data
fpid#-PLANS[-?].PDF	Multi-sheet PDF representing the plan set w/ digital signature(s) applied
fpid#-SPECS[-?].PDF	Specification package
fpid#-SPECS-TSP[BOE item #][-?].PDF	Technical Special Provision

The proposed method is to name the files starting with general information on the left and moving to the more specific on the right.

For example; begin with the FPID#, then the item description (PLANS, SPECS, etc.), then revision or supplement number, and finally any naming specific to the project as specified by the professional of record.

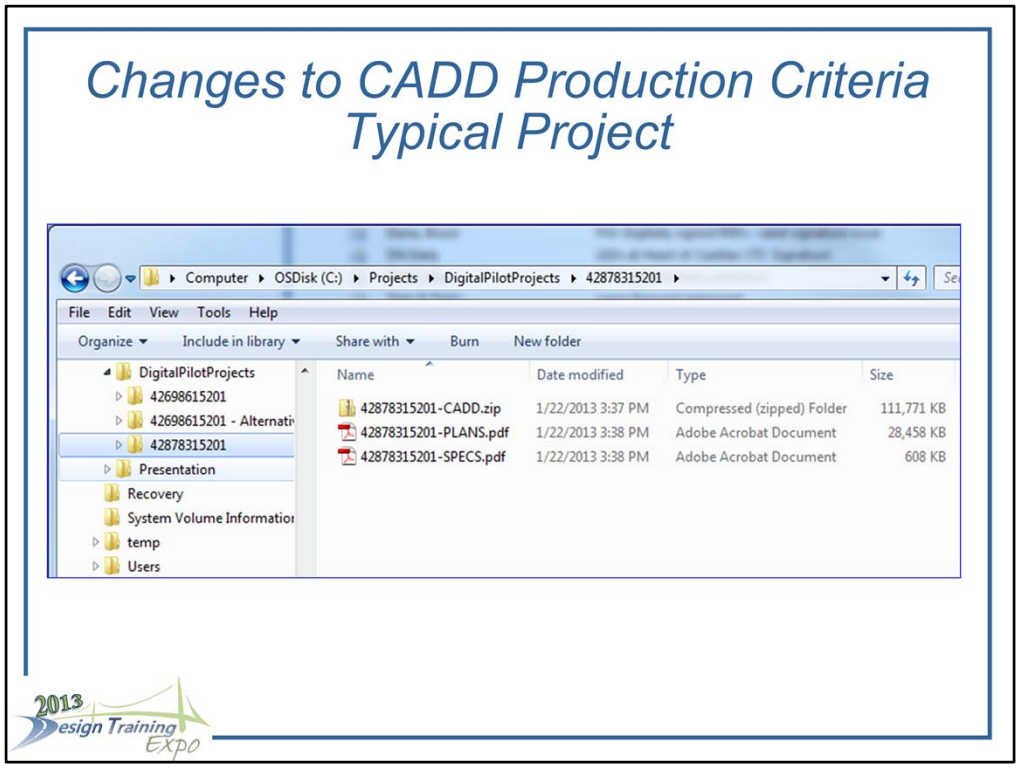
This scheme allows flexibility to name files as they relate to the project. For example, a project that contains multiple bridges may have the bridge numbers as the last characters on the far right. Another example may be a project with major interchanges; the characters to the far right might be an interchange designation. In so doing, the file naming convention guides the downstream consumer of that data in a logical fashion to what it is and how it pertains to the project. This file naming convention allows project files to collate well when they are sorted and combined in a single folder. Text, numbers and dashes are allowed. Characters that interfere with operating system path specifications or XML paths must be excluded (/ \ . : , < & # >). Also exclude underline and spaces. They tend to disappear or interfere when displayed as a URL.

Changes to CADD Production Criteria

Revisions & Supplementals

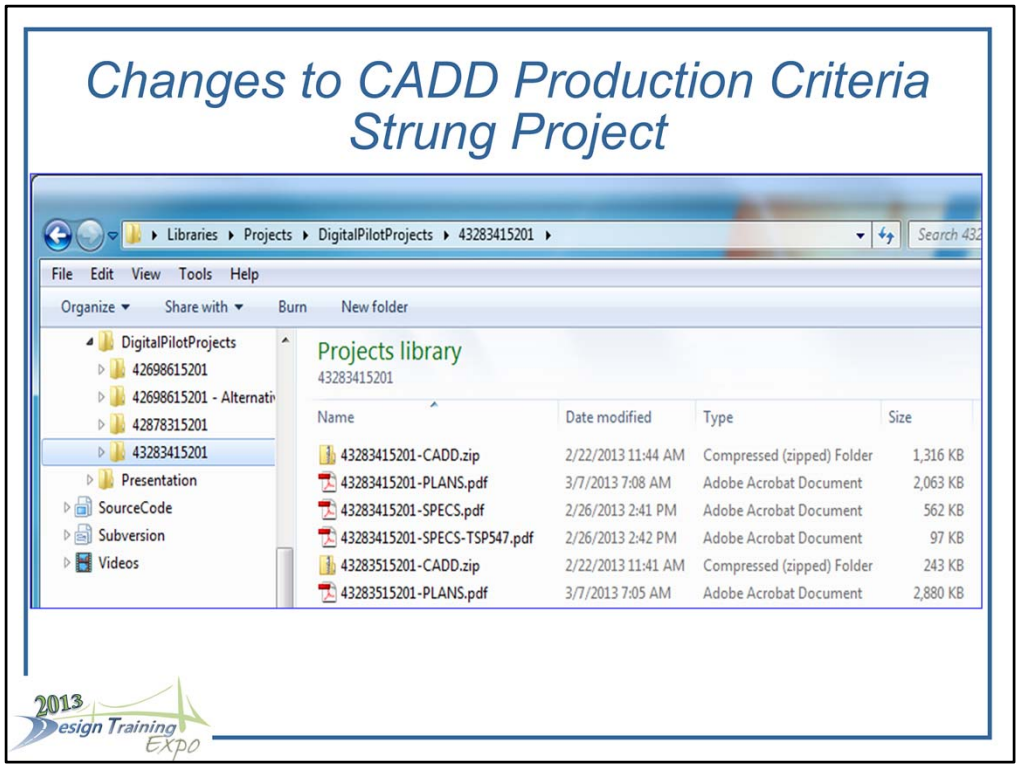
File Name	Contents
fpid#-CADD-REV01[-?].ZIP	Contemporary Native CAD files
fpid#-PLANS-REV01[-?].PDF	Multi-sheet PDF representing only the plan sheets that are revised
fpid#-SPECS-SUPP01[-?].PDF	Supplemental Specification package
fpid#-SPECS-TSP{BOE item #}[-?].PDF	Technical Special Provision

2013 Design Training Expo



This is what the majority of projects will look like

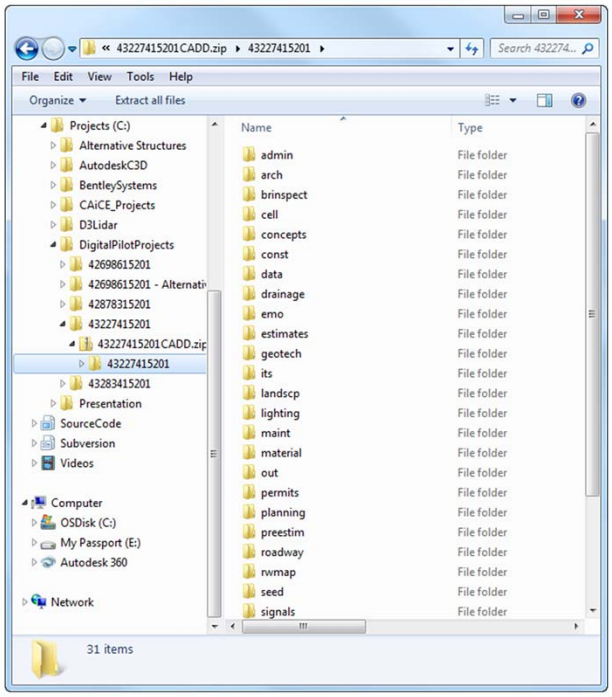
The ZIP file contains the native cad files in the folder structure just the way we always have.



This is what a strung project looks like

Changes to CADD Production Criteria

Content of a Project ZIP retains much of the directory structure and files of the FDOT project directory itself. Non-essential files are culled, and the ZIP process itself will remove empty directories.



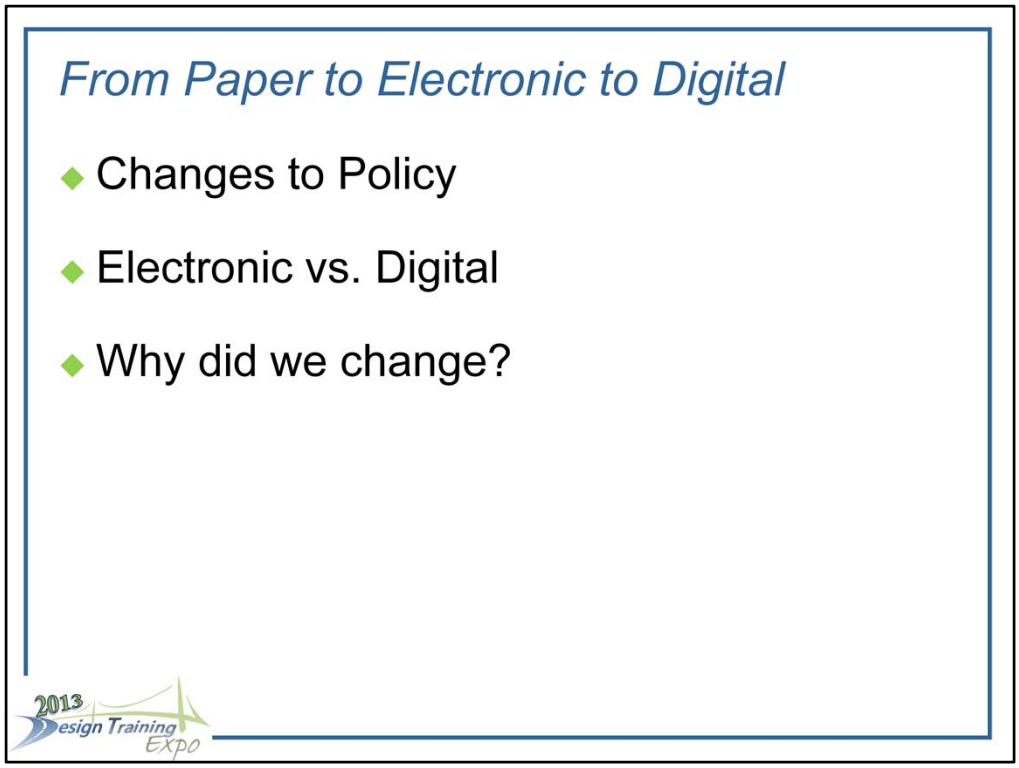
Comparing and Contrasting Classical Electronic Delivery filenames:

Original Delivery	***Revision 1***	***Revision 2***	***Revision 3***
~~ProjectIndex.XML~~	~~ProjectIndex.XML~~	~~ProjectIndex.XML~~	~~ProjectIndex.XML~~
~~Project.PDF~~	~~Project1.PDF~~	~~Project2.PDF~~	~~Project3.PDF~~
~~Sheetndx.HTM~~	~~Sheetndx1.HTM~~	~~Sheetndx2.HTM~~	~~Sheetndx3.HTM~~
	~~Deltandx1.HTM~~	~~Deltandx2.HTM~~	~~Deltandx3.HTM~~
	~~Revison1.PDF~~	~~Revision2.PDF~~	~~Revision3.PDF~~
~~ProjectFiles.HTM~~	~~ProjectFiles.HTM~~	~~ProjectFiles.HTM~~	~~ProjectFiles.HTM~~

to **Digital Delivery** file names:

Original Delivery	***Revision 1/ Supplement1***	***Revision 2/ Supplement1***
fpid-PLANS.PDF	*fpid*-PLANS-REV01.PDF	*fpid*-PLANS-REV02.PDF
fpid-CADD.ZIP	*fpid*-CADD-REV01.ZIP	*fpid*-CADD-REV02.ZIP
fpid-COMPBOOK.PDF	*fpid*-COMPBOOK-REV01.PDF	*fpid*-COMPBOOK-REV02.PDF
fpid-SPECS.PDF *fpid*-SPECS-TSP01.PDF	*fpid*-SPECS-SUPP01.PDF *fpid*-SPECS-TSP01-SUPP01.PDF	*fpid*-SPECS-SUPP02.PDF

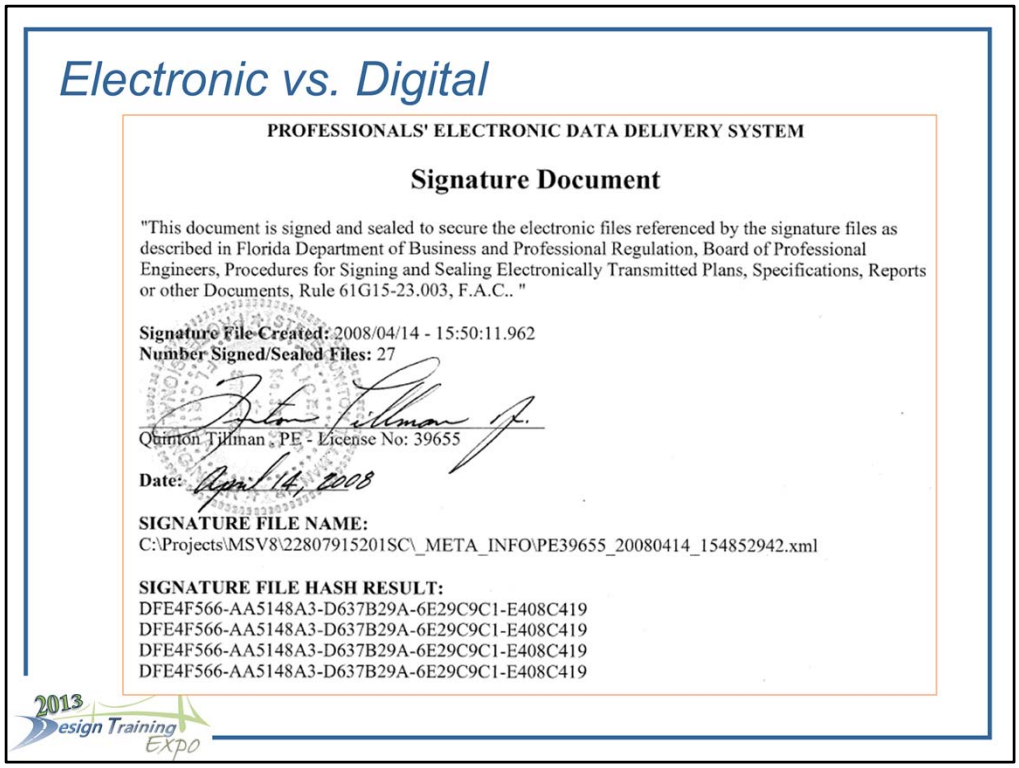
Classical Electronic Delivery Bid Set	*Digital Delivery Bid Set*
Project.pdf represented the plans and is delivered in the project \root folder. Individual sheet image files are created for each sheet in the plans and signed and sealed individually.	***fpid*-PLANS[-].pdf** is a composite PDF of all plan sheets and is capable of being separated from the project \root folder structure. This file is signed and sealed with Digital Signature. Revisions to this file are named: ***fpid*-PLANSREV##[-].pdf** for revisions
The Specifications file was named **fpid.pdf** and retained in the \Specs subfolder of the project.	The Specifications file is named: ***fpid*-SPECS[-].pdf** and is capable of being separated from the project \Specs subfolder. Supplemental Specifications are named: ***fpid*-SPECS-SUPP##[-].pdf**. for supplements
Project "Bid Sets" or "Bid CD's" did not include CADD Data or Engineering data files. The contractor always had to request this data, and often that occurred after award.	Includes a ZIP file, ***fpid*-CADD[-].zip** of the project directory structure containing the CADD and supporting files (Native DGN's or DWG's of the platform used to design the project). **This file is the only file delivered outside and separate from the project folder structure.**. This file is not signed and sealed ! Cull out the unnecessary files that would not benefit the contractor building the project.
SetMaker was used to create the Bid Set from the secured Project CD dataset.	Bid Set file ***fpid*-CADD[-].zip** can be created manually (and should be since only the designer knows which files benefit the contractor and support the plans).
Comp Book was not delivered to the contractor with the Bid Set.	Comp Book is delivered to the contractor and is named ***fpid*-COMPBOOK.pdf** and is capable of being separated from the project folder structure for the bid set. Revisions to the Comp Book are named ***fpid*-COMPBOOKREV##.pdf**



So let's look at the second, Electronic vs. Digital ~ sounds the same.

Defined in the "Electronic Signature Act of 1996"; definitions don't mean much until you are acquainted with the practical application.

"Electronic Signature" is a broad definition – simply means the adoption of electronic symbols that are logically associated with a document with the intent to authenticate its writing. Professionals Electronic Data Delivery System (PEDDS) is an implementation of electronic signature. It maintains list of information about files that an individual intends to sign. PEDDS generates a cryptographic code that uniquely identifies the files from those lists and produces this document.



Anyone who has ever used PEDDS is familiar with this. The electronic files in the list are "signed" by a professional of record when an individual strokes a wet ink signature and applies a professional seal. The applicable language from FAC on the document asserts the individuals intent to sign the files. This document tells us two things, the identity of the individual signing the files and a cryptographic result representing the files he intended to sign. An individual receiving these files can then use the PEDDS software along with this paper document to authenticate the files. Without this paper "Signature Document" there is no way to truly authenticate the files. This resulted in a substantial reduction in the volume of paper; however, we still rely on a wet ink signature on paper.

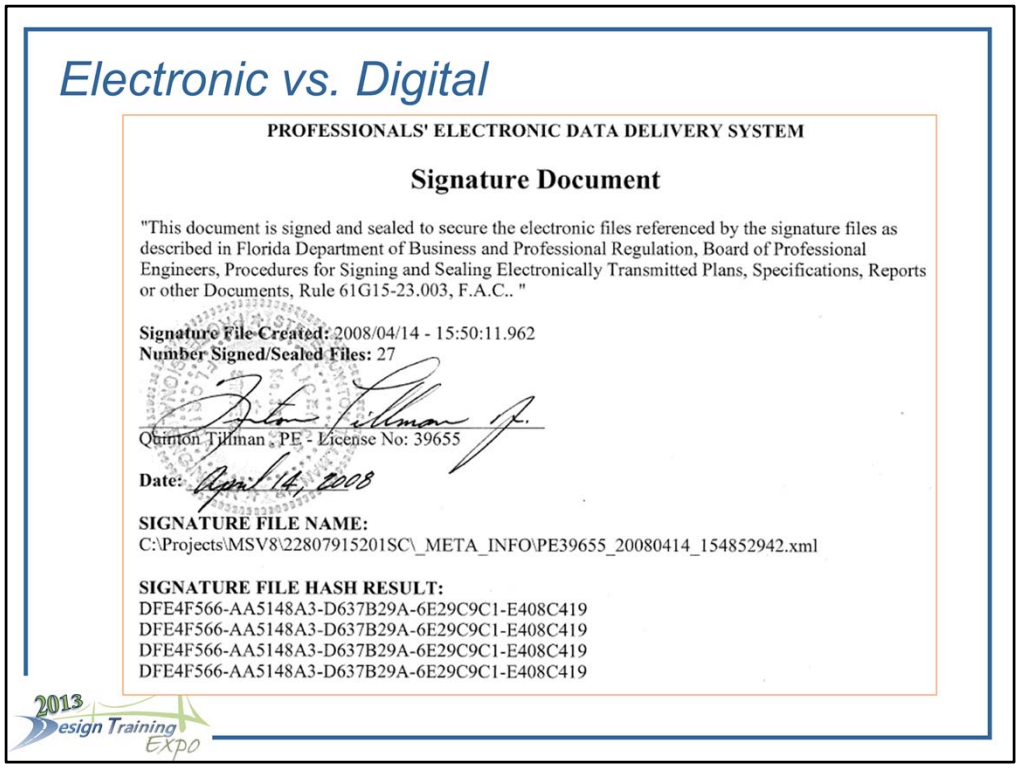
Security Services

- **Data integrity** services address the unauthorized or accidental modification of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect unauthorized data modification. The goal is for the receiver of the data to verify that the data has not been altered.
- **Confidentiality** services restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the unauthorized disclosure of information to unauthorized individuals or processes.
- **Identification and authentication** services establish the validity of a transmission, message, and its originator. The goal is for the receiver of the data to determine its origin.
- **Non-repudiation** services prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

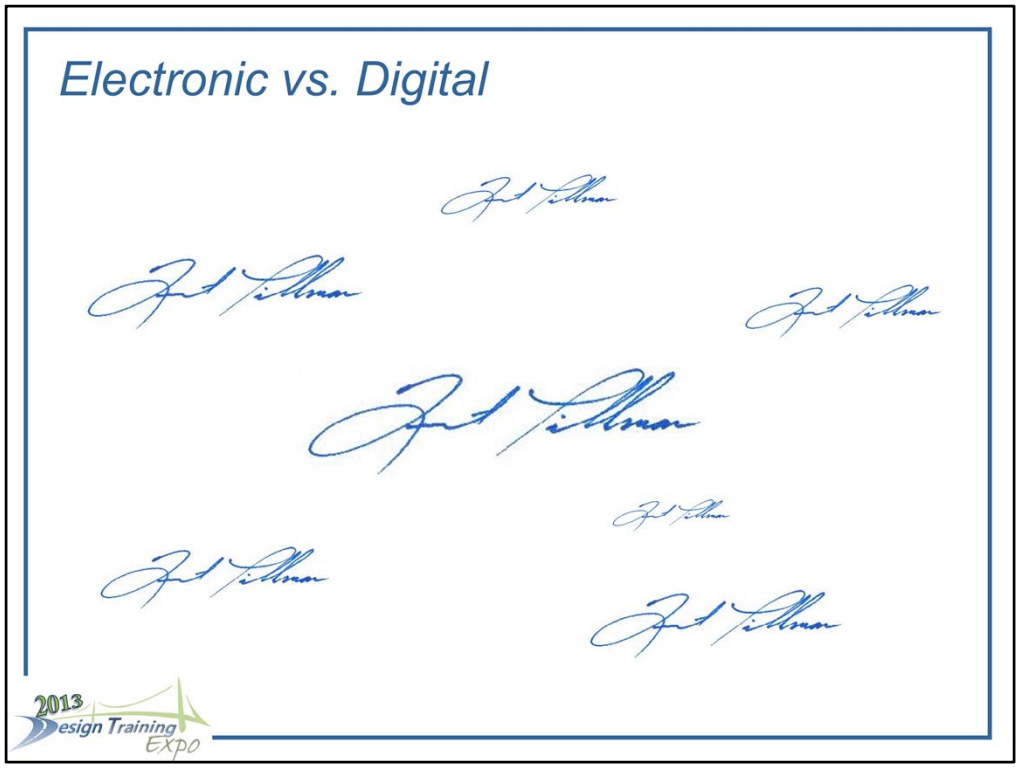
Publication SP 800-32, National Institute of Standards and Technology, 2001. U.S. Government publication.

2013 Design Training Expo

The National Institute of Standards and Technology (NIST) classify four basic services provided by electronic signature.
Data integrity – has anything been modified, any new data inserted or anything deleted.
Confidentially – restricts access. Projects are transmitted by completely unsecured means
Identification and authentication – Who is the originator of the data?
Non-repudiation – receiver can know with reasonable confidence the identity of the individual signing the data. Prevents an individual from denying that previous actions were performed.
We are primarily interested in three of these that PEDDS provides.



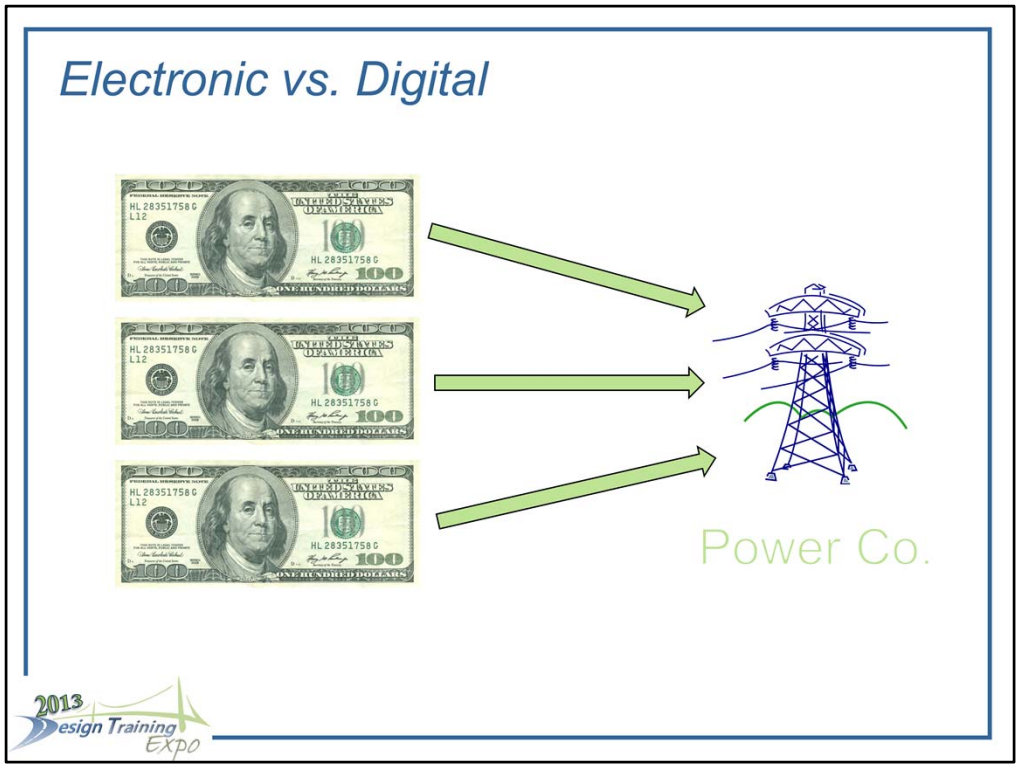
So let’s go back and look at our Signature Document
For centuries a wet ink signature on paper has been the most viable means of verifying ones approval, consent or authorship of a variety of documents. Everything from proclamations and declarations to legal contracts to personal letters are signed with a signature.
Science behind handwritten signatures.



What is this? Is it a digital signature?
Digitized signature – not to be confused with a digital signature
Digitized signature is simply a non-cryptographic signature. It offers nothing in the way of any of the services on the previous slide. There is absolutely no verification or non-repudiation.
Allow me to use another example to illustrate my point. $100 bill intrinsic value

Electronic vs. Digital

Image of a $100 bill – it has no value.



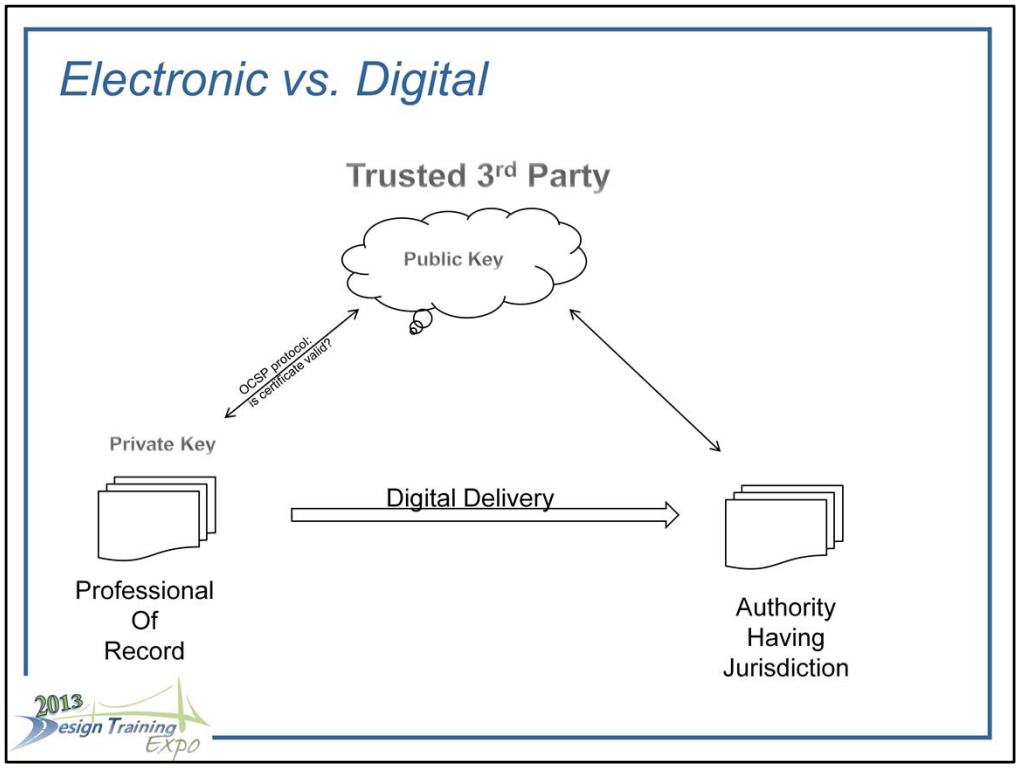
Pay the power company with an image – hardly!

By the same reasoning, a digitized image of a signature has no means of data integrity, no means of verification and certainly no non-repudiation.
Our first implementation of electronic signature was complete in 1998. The mantra at the time was “Don’t let the technology change our business practices!” PEDDS was a half-step towards a totally electronic solution. It produced single files that were images of paper plan sets and relied upon a wet ink signature on paper.
As we move away from wet ink signature or intent is to adopt methods that give the same level of assurance, if not better, for verification of authenticity of a document that we once had with wet-ink signature and seal.

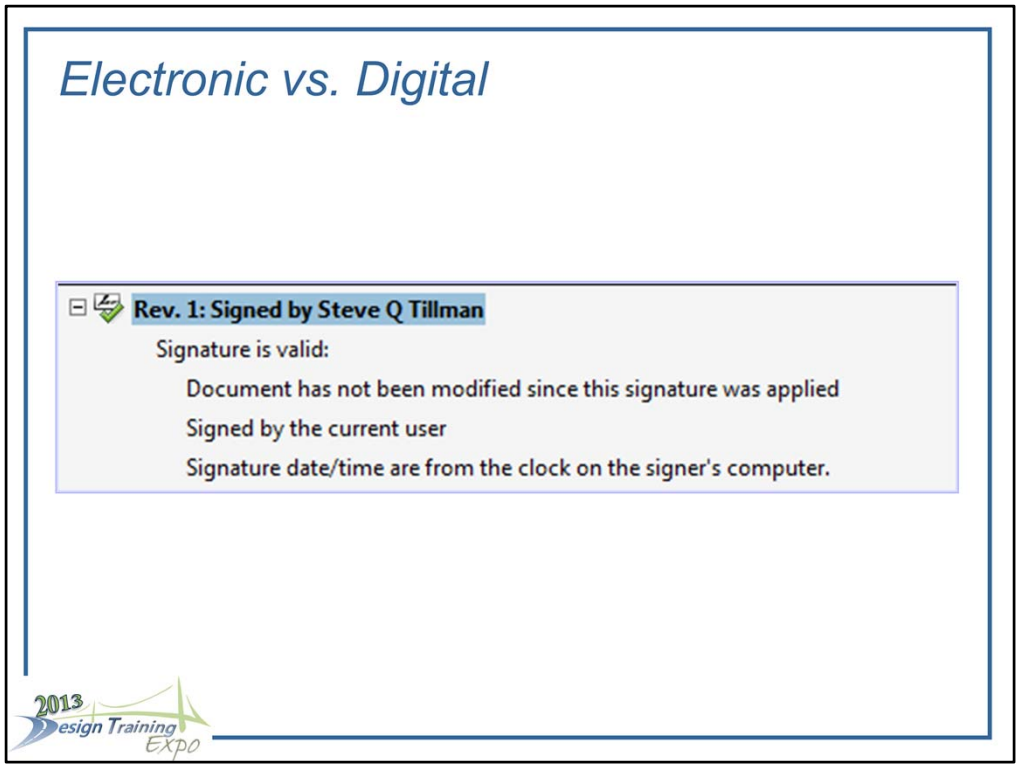
Electronic vs. Digital

- Non-Cryptographic security mechanisms
  - ✓ Digitized image of signature
- Symmetrical Key Cryptography
  - ✓ Old method with PEDDS
  - ✓ Paper reports
- Asymmetrical Cryptography
  - ✓ New method Public Key Cryptography
  - ✓ Paperless

We have looked at non-cryptographic, digitized signature – not useful for our purposes. Symmetrical, electronic signature, old process, PEDDS. Asymmetrical, digital signature, new process.



Digital signature work quite differently than PEDDS. Cryptographic information is embedded in the file to be signed sealed and secured. Remember PEDDS only reads files and maintains list of information. Digital signature actually alters the files! This has significant implications throughout the delivery process.



Document is valid when the cryptographic keys match. Look at the security services again.

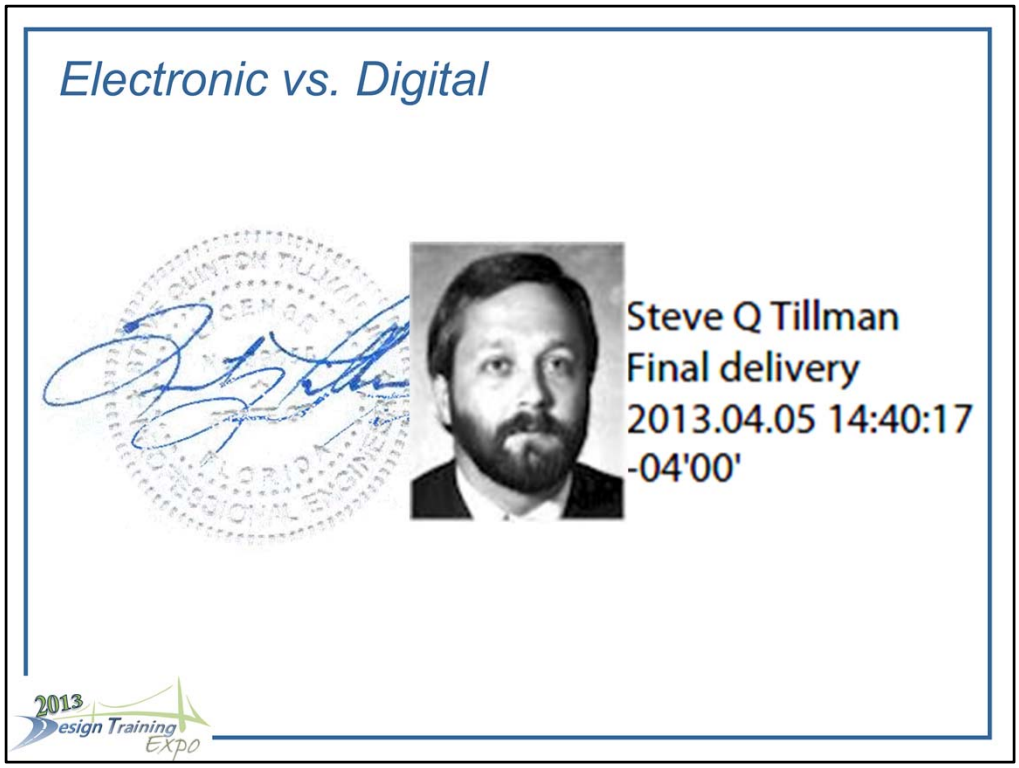
Security Services

- **Data integrity** services address the unauthorized or accidental modification of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect unauthorized data modification. The goal is for the receiver of the data to verify that the data has not been altered.
- **Confidentiality** services restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the unauthorized disclosure of information to unauthorized individuals or processes.
- **Identification and authentication** services establish the validity of a transmission, message, and its originator. The goal is for the receiver of the data to determine its origin.
- **Non-repudiation** services prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

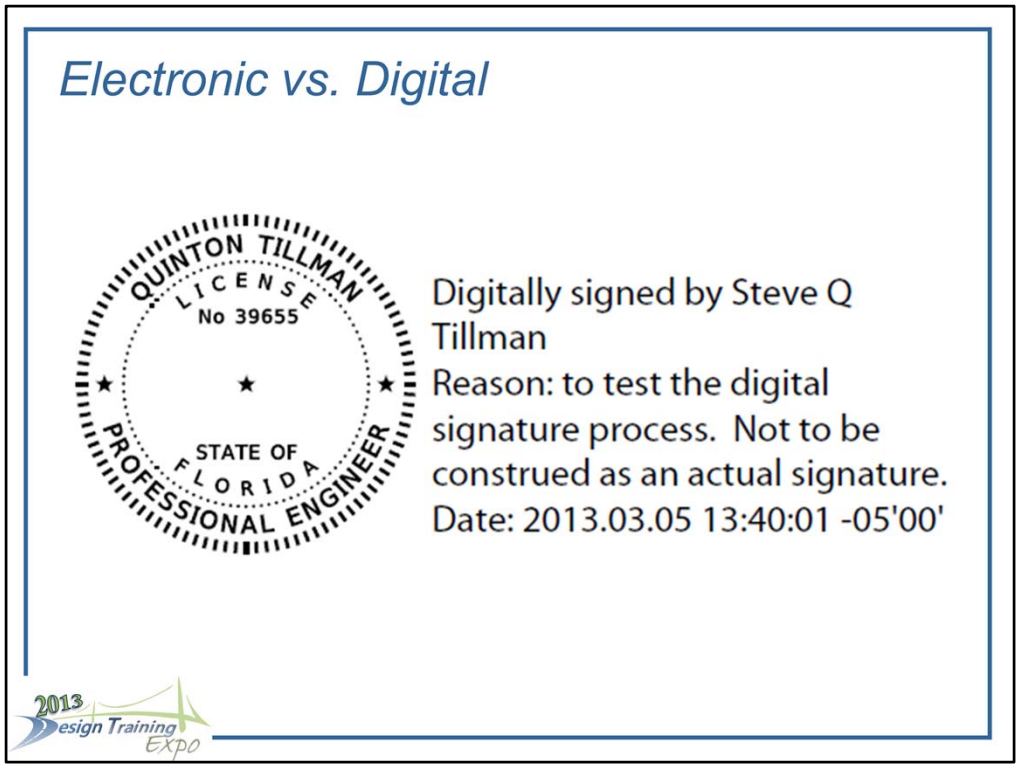
Publication SP 800-32, National Institute of Standards and Technology, 2001. U.S. Government publication.

2013 Design Training Expo

Same services that we had with PEDDS signature document



Digital signature can apply a digital appearance. Remember the digitized signature earlier, it's only an appearance. The actual security services are provided by the underlying cryptography. When writing procedures don't get too hung-up with the appearance.



This is the appearance that we have settled on thus far. Nothing sacred about it.

Access Certificates for Electronic Services (ACES)

- ACES program - created and sponsored by the GSA
- Facilitate secure on-line access to information and services through PKI and digital signature technology
- Business-2-Government , Consumer-2-Government Transactions.
- “Real Time” validation
- Digital Signatures on electronically produced documents and forms which are non-reputable.

Why did we choose the type of digital certificate that we did.

Access Certificates for Electronic Services.

There are many different services

Appropriate Certificate Uses

Assurance Level	Appropriate Certificate Uses
Rudimentary	Lowest degree of assurance concerning identity of the individual.
Basic	Used where risks and consequences of data compromise are not considered to be of major significance.
Medium	Environments where risks and consequences of data compromise are moderate. Transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
PIV-I Card Authentication	Similar to Medium, may include smart card and reader where PIN
Medium Hardware	This may include very high value transactions or high levels of fraud risk.
High	Reserved – Government environments

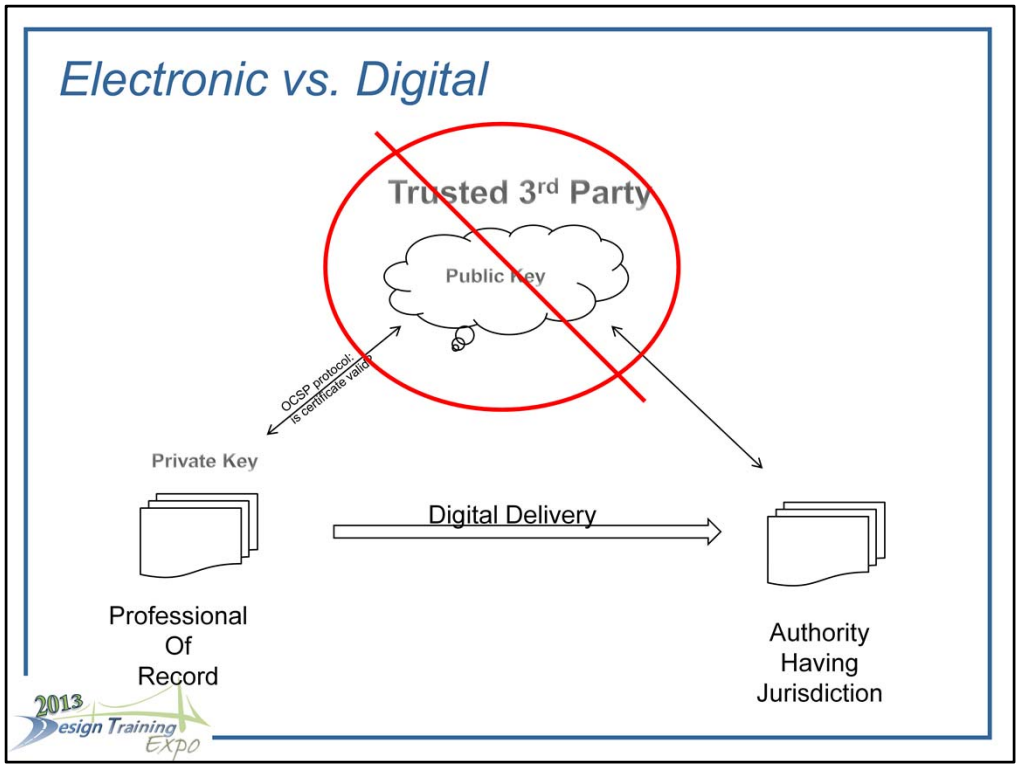
2013 Design Training Expo

X.509 Certificate Policy for the FBCA, Ver 2.25, December 9,2011

Levels of security

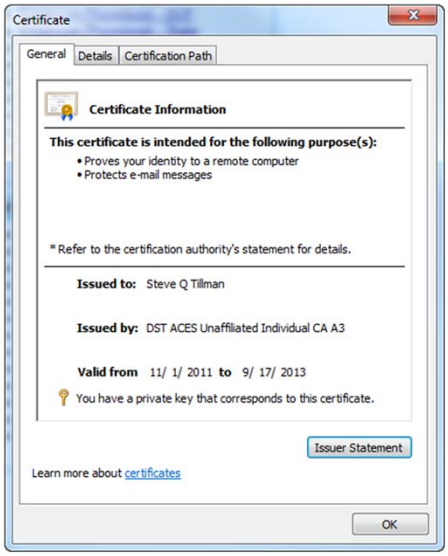
Anonymity – Who are you?

On the Internet, nobody knows you're a dog!

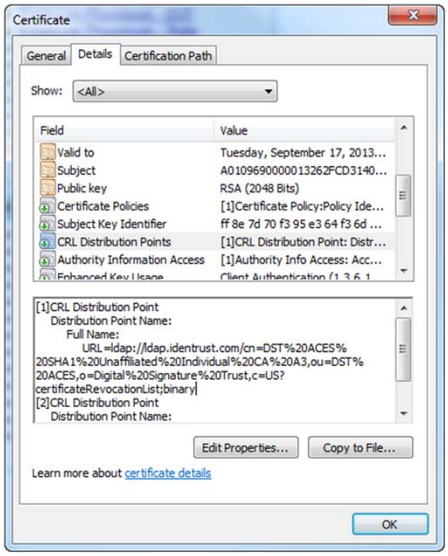

Electronic vs. Digital
Trusted 3rd Party
Public Key
OCSP protocol:
is certificate valid?
Private Key
Digital Delivery
Professional
Of
Record
Authority
Having
Jurisdiction
2013
Design Training
Expo

Electronic vs. Digital

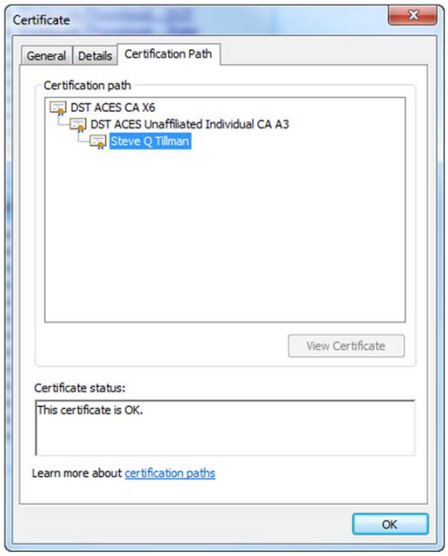
X.509 Certificate Information



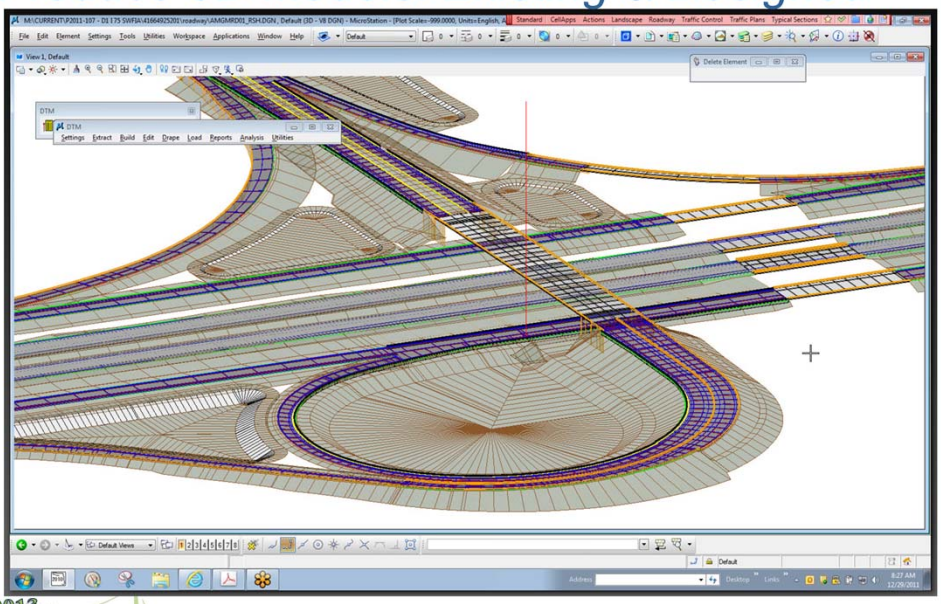
X.509 Certificate Information



X.509 Certificate Information



Produce 3D Models: Existing & Designed



2013 Design Training Expo

Electronic Signature Act of 1996

- Facilitate economic development and efficient delivery of government services by means of reliable electronic messages.
- Enhance public confidence in the use of electronic signatures.
- Minimized the incidence of forged electronic signatures and fraud in electronic commerce.
- Foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to writings in any electronic medium.
- Assure that proper management oversight and accountability are maintained for agency conducted electronic commerce.

2013 Design Training Expo

The legislative intent

From Paper to Electronic to Digital

- Changes to Policy
- Electronic vs. Digital
- Why did we change?

Why did we change?

- Known difficulty with current process.
- Disadvantages with current process.
- Better security practices.
- The time has come.

Why did we change?

Florida Department of Transportation

Engineering / CADD Systems Office

Phone: (850) 245 – 1600

Email: ecso.support@dot.state.fl.us

BRUCE DANA, P.E.
QUINTON TILLMAN, P.E.

2013 Design Training Expo

Security Services

- **Data integrity** services address the unauthorized or accidental modification of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect unauthorized data modification. The goal is for the receiver of the data to verify that the data has not been altered.
- **Confidentiality** services restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the unauthorized disclosure of information to unauthorized individuals or processes.
- **Identification and authentication** services establish the validity of a transmission, message, and its originator. The goal is for the receiver of the data to determine its origin.
- **Non-repudiation** services prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

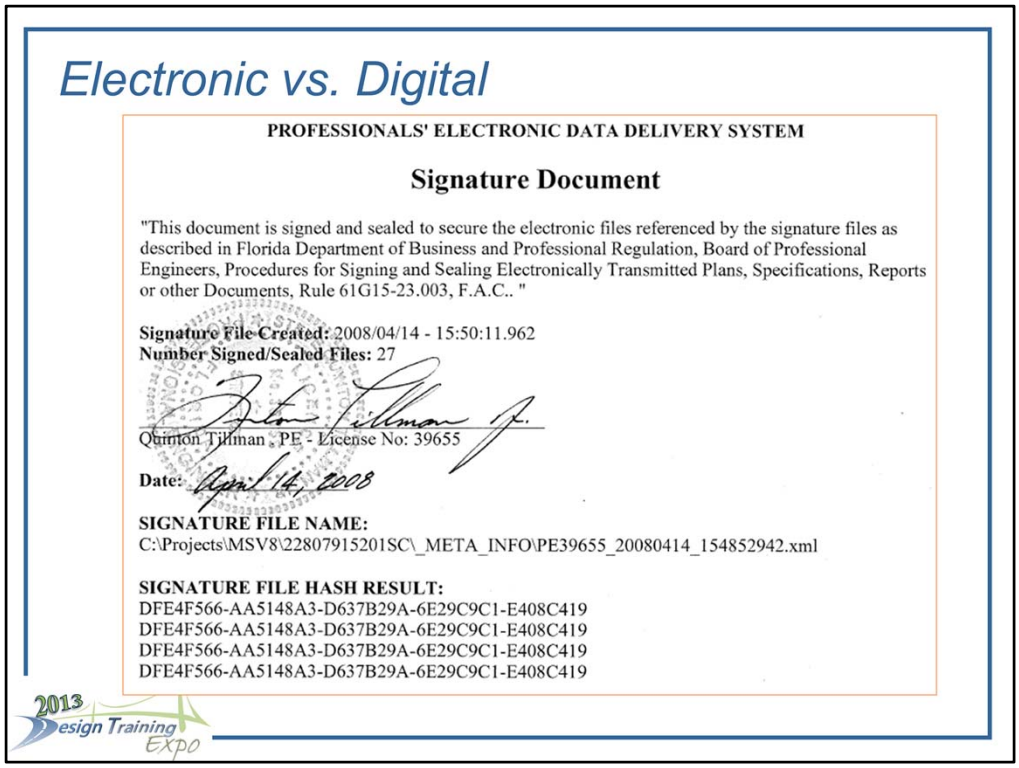
Publication SP 800-32, National Institute of Standards and Technology, 2001. U.S. Government publication.

2013 Design Training Expo

The National Institute of Standards and Technology (NIST) classify four basic services provided by electronic signature. We are primarily interested in three of these that PEDDS provides. We just saw these on the previous slide.

Projects are transmitted by completely unsecured means, PEDDS authentication process tells us if anything changed. There are unintended consequences.

For centuries a wet ink signature on paper has been the most viable means of verifying ones approval, consent or authorship of a variety of documents. Everything from proclamations and declarations to legal contracts to personal letters are signed with a signature.



So let’s go back and look at our Signature Document

We know whonthis person is by their handwritten signature.

Why do we go thru this amount of effort and trouble?

Anonymity – Who are you?

On the Internet, nobody knows you're a dog!

What is this? Is it a digital signature?

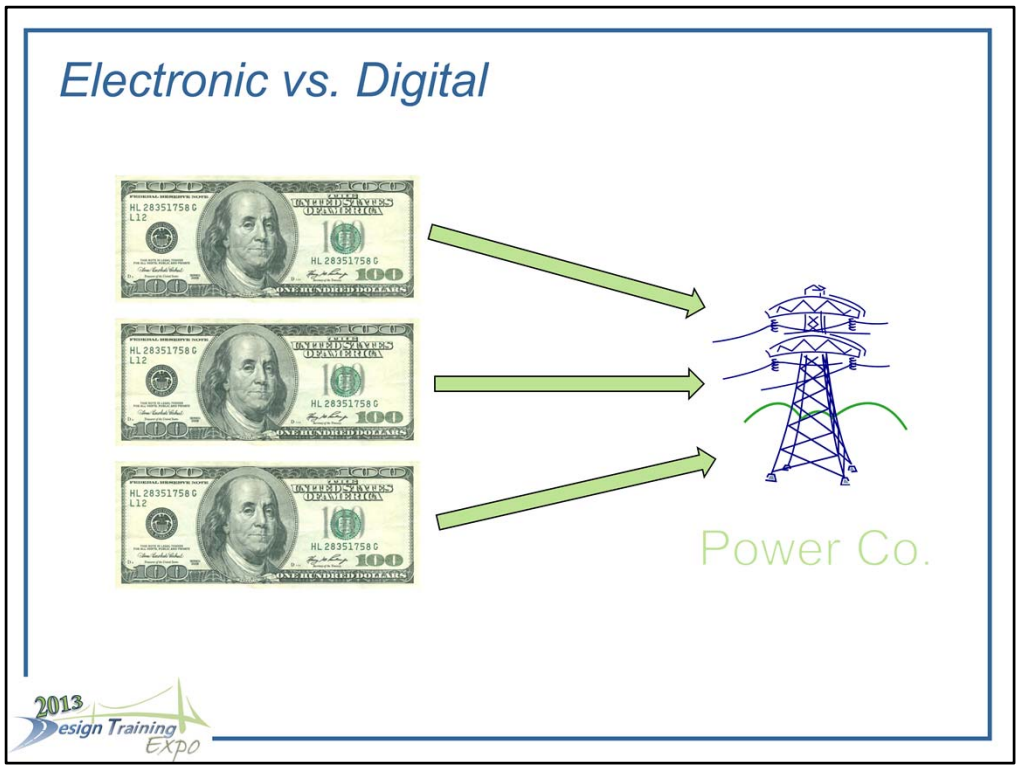
Digitized signature – not to be confused with a digital signature.

Digitized signature is simply a non-cryptographic signature. It offers nothing in the way of any of the services on the previous slide. There is absolutely no verification or non-repudiation.

Our first implementation of electronic signature was complete in 1998. The mantra at the time was “Don’t let the technology change our business practices!” PEDDS was a half-step towards a totally electronic solution.

As we move away from wet ink signature or intent is to adopt methods that give the same level of assurance, if not better, for verification of authenticity of a document that we once had with wet-ink signature and seal.

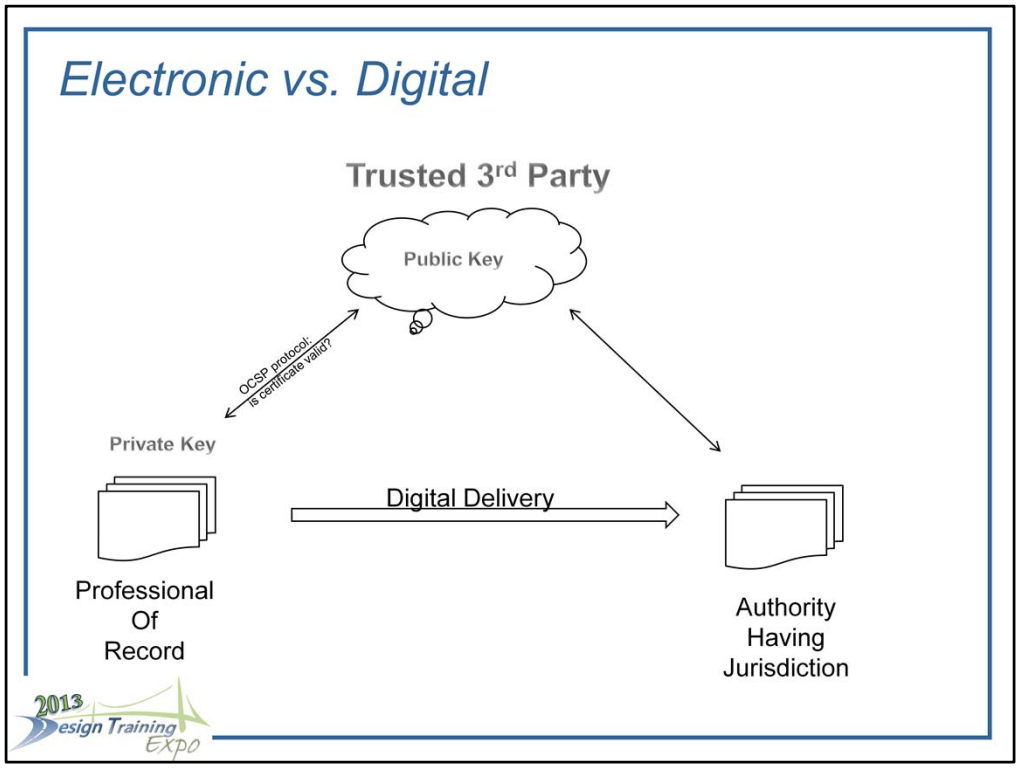
Electronic vs. Digital


Electronic vs. Digital
Power Co.
2013 Design Training Expo

Electronic vs. Digital

- Non-Cryptographic security mechanisms
  - ✓ Digitized image of signature
- Symmetrical Key Cryptography
  - ✓ Old method with PEDDS
  - ✓ Paper reports
- Asymmetrical Cryptography
  - ✓ New method Public Key Cryptography
  - ✓ Paperless

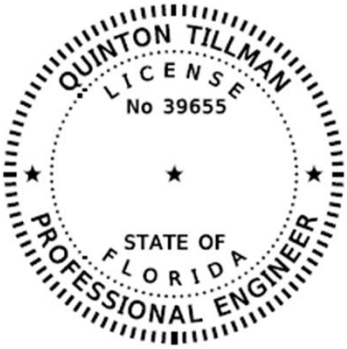
We have looked at non-cryptographic, digitized signature – useless


Electronic vs. Digital
Trusted 3rd Party
Public Key
OCSP protocol:
is certificate valid?
Private Key
Digital Delivery
Professional
Of
Record
Authority
Having
Jurisdiction
2013
Design Training
Expo

Electronic vs. Digital

Steve Q Tillman
Final delivery
2013.04.05 14:40:17
-04'00'

Electronic vs. Digital



Digitally signed by Steve Q Tillman
Reason: to test the digital signature process. Not to be construed as an actual signature.
Date: 2013.03.05 13:40:01 -05'00'

Electronic vs. Digital

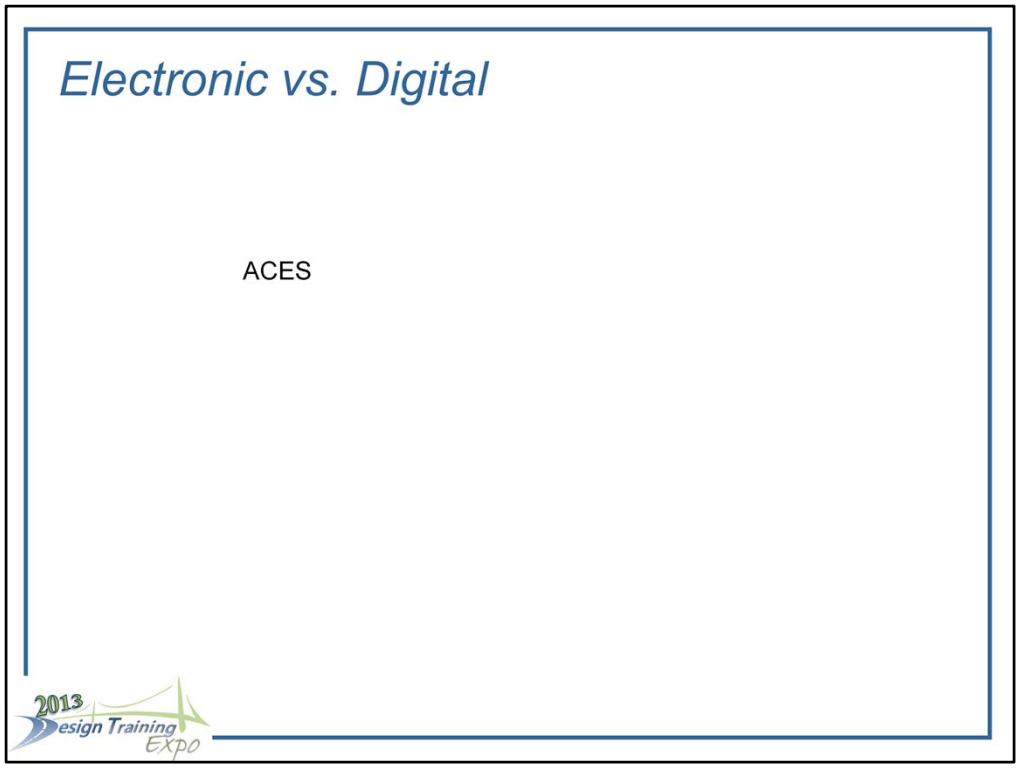
Rev. 1: Signed by Steve Q Tillman

Signature is valid:

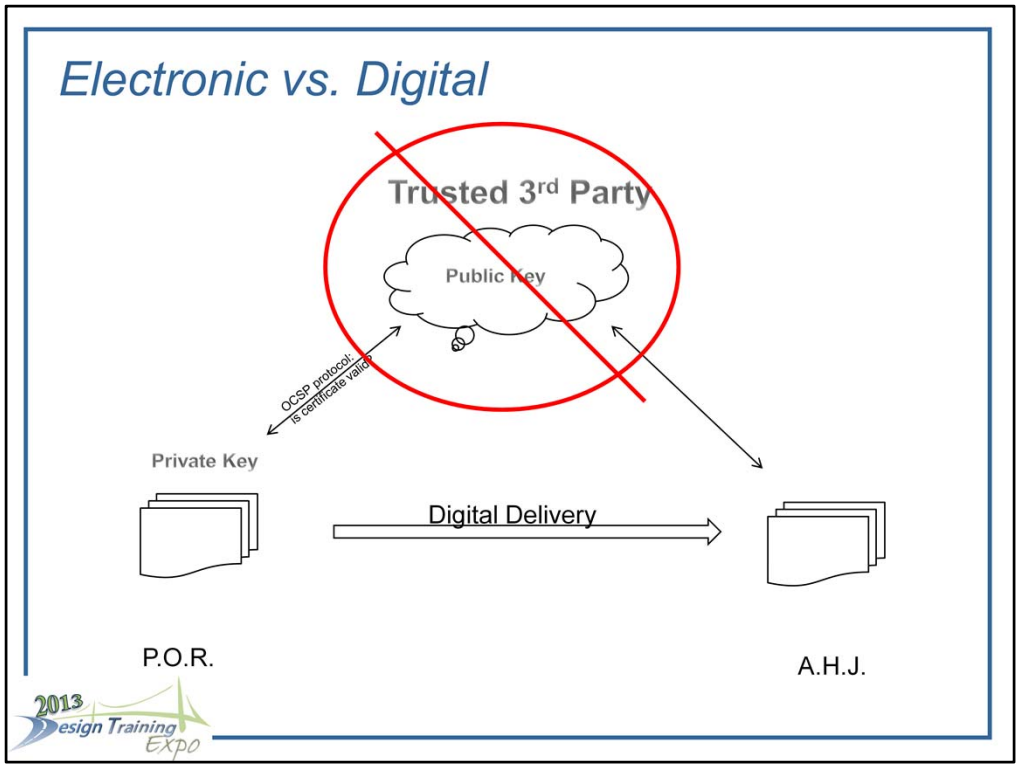
Document has not been modified since this signature was applied

Signed by the current user

Signature date/time are from the clock on the signer's computer.



Why did we choose the type key that we did.


Electronic vs. Digital
Trusted 3rd Party
Public Key
OCSP protocol:
is certificate valid?
Private Key
Digital Delivery
P.O.R.
A.H.J.
2013
Design Training
Expo

Electronic vs. Digital

Electronic Signature Act of 1996

- Facilitate economic development and efficient delivery of government services by means of reliable electronic messages.
- Enhance public confidence in the use of electronic signatures.
- Minimized the incidence of forged electronic signatures and fraud in electronic commerce.
- Foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to writings in any electronic medium.
- Assure that proper management oversight and accountability are maintained for agency conducted electronic commerce.

The legislative intent

From Paper to Electronic to Digital

- Changes to Policy
- Electronic vs. Digital
- Why did we change?

Why did we change?

- Known difficulty with current process.
- Disadvantages with current process.
- Better security practices.
- We were directed to!

Why did we change?

Florida Department of Transportation

Engineering / CADD Systems Office

Phone: (850) 245 – 1600

Email: ecso.support@dot.state.fl.us

BRUCE DANA, P.E.
QUINTON TILLMAN, P.E.