DECEMBER 16, 2019

ELECTRONIC PERMITTING GUIDE:
ON-LINE SUBMITTAL FOR DESIGN PROFESSIONALS

Provided by:
COLLIER COUNTY GROWTH MANAGEMENT DEPARTMENT
CITY OF NAPLES BUILDING DEPARTMENT
CITY OF MARCO ISLAND BUILDING SERVICES DIVISION

ELECTRONIC PERMITTING GUIDE:
ON-LINE SUBMITTAL FOR DESIGN PROFESSIONALS

Building, Planning and Zoning Departments across the country are moving rapidly toward paperless submittal of design professional's signed & sealed documents. This guide was created collaboratively by the City of Naples, Marco Island and Collier County to clarify, and where possible standardize, our requirements for electronic submittal.

WHO MUST USE A DIGITAL SIGNATURE TO SUBMIT ELECTRONICALLY?

Professional Engineers, Architects, Landscape Architects, Interior Designers and Surveyors

Florida Administrative Code References:

- 61G15: Board of Professional Engineers, Chapter 23: Seals, Rules 23.004-23.005 were updated effective 6/19/2018.
- 61G1: Board of Architecture and Interior Design, Chapter 16: Seals and Plans, last updated 11/11/2013.
- 61G10: Board of Landscape Architecture, Chapter 11: Licensure, Rule 11.011 was last updated 2/16/2006.
- Chapter 5J-17: Board of Professional Surveyors and Mappers, Rule 5J-17.062 was last updated 12/16/2007.

Building Official's Interpretation:

Professional Engineers must obtain Digital Signatures from a Certificate Authority

- The updated rule for Engineers, *61G15-23.004: Procedures for Digitally Signing and Sealing Electronically Transmitted Plans, Specifications, Reports or Other Documents*, requires that the professional engineer "shall have their identity authenticated by a certification authority". As defined in F.S. 668.003(2), a "certification authority" means a person who issues a certificate.
    - Our Building Officials interpret this change as a requirement to use a third-party verification entity, the certificate authority, to certify the engineer's identity.
- All other design professionals may either obtain a digital signature from a certification authority (a third-party entity) or create a signature in a software application like Adobe (a self-signed certificate).

WHAT WE HAVE LEARNED ABOUT RECEIVING DIGITALLY SIGNED DOCUMENTS TO DATE

Signature Authorities:

Local Design Professionals have successfully submitted documents using these Certificate Authorities –

- Cosign – http://www.arx.com/digital-signature/
- DocuSign - https://www.docusign.com/products/electronic-signature
- Entrust - https://www.entrust.com/document-signing-certificates/
- Globalsign – https://www.globalsign.com/en/digital-signatures/
- VeriSign - https://www.symantec.com/products/information-protection/eca-certificates/pricing “
- Digicert - https://www.digicert.com/document-signing/

Document Security:

Digitally signing your design file protects the contents from being altered. Please do not add any additional/optional security from your pdf software or certification authority. “Locking” or “Restricting” the document before you submit the file can prevent us from opening and processing the document or stamping it for approval in our software. This results in lost time for us all and may require you to submit a new set of documents.

Combining PDF Documents:

PDF binders are the preferred method of combining sheets. Please do not use PDF Portfolios to combine sheets. PDF Portfolios are not compatible with our permitting software and will require for the files to be recreated in order to be processed into review. Also, please do not combine pdf files that have been separately digitally signed and sealed, as this invalidates the digital signatures and does not allow for us to process the document into review.

Understanding Professionally Sealed Sheets vs. Digitally Signed Files

We require design documents to be submitted as one digitally signed file, per signer.

Adding a visual representation of your professional seal and signature to each page of your design is always acceptable; you can do this with a stamp in your pdf software or by copying and pasting the image on your document pages. Please do not affix a digital signature to each page.

WHAT DO ALL THESE NEW TERMS MEAN?

Digital Signature:

- A type of electronic signature that uses algorithms to transform your document in a way that allows the recipient to verify the document was signed by you and that the sealed document contents have not been changed.
- The algorithms perform two tasks; creating the message digest or "hash" of your document, then using your "private key" to bind the hash, digital certificate and signature to the document. The recipient then uses the "public key" to check the submittal hasn't been altered.

Electronic Signature:

- Symbols or other data in digital form attached to an electronically transmitted document as verification of the sender's intent to sign the document.
- Algorithms are not used to "hash" the document, so verification of document integrity is not available.

Key Pairs/PKI:

- Through PKI (Public Key Infrastructure), each digital signature transaction includes a pair of keys. The private key is unique to the individual signing the document and must be kept secure. The public key is openly available and used to validate the signer's identity.
- PKI enforces other requirements such as Certificate Authorities (CA's) and digital certificates.

Certificate Authority:

- A Certificate Authority (CA) is a trusted entity that issues Digital Certificates and public-private key pairs.
- The role of the Certificate Authority (CA) is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be.

Digital Certificate:

- The digital certificate is an essential part of secure communication. It includes the owner's public key, the expiration date of the certificate, the owner's name, certificate issuing authority and other information.
- The certificate travels with your document electronically. When the recipient opens the document in their pdf software, it runs a validation check on the

signature and document content, checks the signing date and certificate expiration date, and accepts or rejects the signature as authenticated.

Algorithm/Hash:

- Secure Hash Algorithms are a family of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard.
- The algorithm takes an input, your document, and produces a message digest, the hash value. The SHA-1 standard produces a hash value typically rendered as a hexadecimal number, 40 digits long!

DO ALL DIGITAL SIGNATURES SOURCES PROVIDE THE SAME SERVICES?

No, they provide different levels of security and ease of use

Know What You Are Buying from a Certificate Authority:

- Some 3rd Party vendors offer both Digital and Electronic Signatures. All design professionals in Florida must use a Digital Signature; digital signatures utilize the hash algorithms that meet the FAC requirement for validating document integrity.
- Certificate Authorities may provide your credentials different ways.
    - Some provide digital certificates on USB dongles or smart cards. This provides better security for your private key and allows you to work from more than one location.
    - Others provide a certificate file to download and save on your workstation.
- Make sure your Digital Certificate will clearly identify the Issuing Authority and their Root Certificates.

How Is A Self-Signed Digital Certificate Different?

- You can create a Digital Signature yourself in pdf software programs like Adobe and Bluebeam.
    - Like a 3rd Party Certificate, it runs a hash algorithm and creates key pairs.
    - But there is no outside validation that the digital signature was in fact created by you. Anyone who can see your license number on a set of plans can create a digital signature and submit documents as you!

- Generally, you create a signature in a specific software program on a specific computer. If you create a signature on a second computer, your laptop perhaps, it will have a *different* Digital Certificate.
- Self-Signed Digital Certificates must be loaded in a “certificate store” on the recipients end to validate properly. 3rd Party certificates do not require this step.