Introduction:

The St. Johns River Water Management District (the District) provided electronic permitting in 2004. When implemented, the District adopted the method described in paragraph 4 (now paragraph 3) of the 61G15 Florida Administrative Code, section 23.003. The District now accepts PKI digitally signed documents, as described in paragraph 2 of the 61G15 Florida Administrative Code.

Note: Since this initial feature implementation, the Florida Administrative Code, Chapter 5J-17, has also been modified to allow for electronic signing and sealing of survey reports.

61G15-23.003

The contents of these paragraphs and the explanation of how the District meets the requirements of 61G15 are provided here.

Paragraph 2

(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.

Rulemaking Authority 471.025(1), 668.006 FS. Law Implemented 471.025 FS. History–New 8-18-98, Amended 9-4-05, 5-6-09.

Description:

The role of a certificate authority is to issue and revoke certificates as required to ensure the integrity of signatures for engineering professionals, and to provide for non-repudiation of the electronic signature. Several digital signature products are now available in the public market. These products meet each of the requirements listed in paragraph 2. Although the District does not endorse or recommend any special product, examples of products that meet the 61G15 Florida Administrative Code requirements can be found at:

- Adobe
- Entrust
- GlobalSign

Definitions:

Digitally Signed:

A digitally “signed” document usually displays a green check mark signature. Once a document has been signed, someone can modify the document, but if they do, the graphic on the signature changes (usually a red x) to indicate that the document has been modified since signing.

Digitally Certified:

Documents can also be “certified.” This generally displays a blue ribbon signature. The person certifying the document can allow people to add signatures after the document is certified, but people can only change what the certifier allows. For example, one person might certify the document, but others add their signatures to sign off on various pages in the document.

Paragraph 3

(4) Alternatively, electronic files may be signed and sealed by creating a “signature” file that contains the engineer’s name and PE number ***(Item 1)***, a brief overall description of the engineering documents ***(Item 2)***, and a list of the electronic files to be sealed ***(Item 3).***

Each file in the list shall be identified by its file name utilizing relative Uniform Resource Locators (URL) syntax described in the Internet Architecture Board’s Request for Comments (RFC) 1738, December 1994, which is hereby adopted and incorporated by reference by the Board and can be obtained from the Internet Website: ftp://ftp.isi.edu/ in-notes/rfc1738.txt. ***(Item 6)***

Each file shall have an authentication code defined as an SHA-1 message digest described in Federal Information Processing Standard Publication 180-1 “Secure Hash Standard,” 1995 April 17, which is hereby adopted and incorporated by reference by the Board and can be obtained from the Internet Website: http://www.itl.nist.gov./div897/pubs/fip180-1.htm. ***(Item 4)***

A report shall be created that contains the engineer’s name and PE number, a brief overall description of the engineering documents in question and the authentication code of the signature file. This report shall be printed and manually signed, dated, and sealed by the professional engineer in responsible charge. ***(Item 5)*** The signature file is defined as sealed if its authentication code matches the authentication code on the printed, manually signed, dated and sealed report. Each electronic file listed in a sealed signature file is defined as sealed if the listed authentication code matches the file’s computed authentication code.

Rulemaking Authority 471.025(1), 668.006 FS. Law Implemented 471.025 FS. History–New 8-18-98, Amended 9-4-05, 5-6-09.

5J-17.062

The contents of these paragraphs and the explanation of how the District meets the requirements of 5J-17.062 are provided here.

Paragraph 3

(3) An electronic signature is a digital authentication process attached to or logically associated with an electronic document and shall carry the same weight, authority, and effect as an original signature and raised seal. The electronic signature, which can be generated by using either public key infrastructure or signature dynamics technology, must be as follows:

(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 manner that the electronic signature is invalidated if any data in the document are changed.

Rulemaking Authority 472.008, 472.025 FS. Law Implemented 472.025 FS. History–New 2-1-00, Amended 12-16-07, Formerly 61G17-7.0025.

Description:

The role of a certificate authority is to issue and revoke certificates as required to ensure the integrity of signatures for engineering professionals, and to provide for non-repudiation of the electronic signature. Several digital signature products are now available in the public market. These products meet each of the requirements listed in paragraph 2. Although the District does not endorse or recommend any special product, examples of products that meet the 61G15 Florida Administrative Code requirements can be found at:

- Adobe
- Entrust
- GlobalSign

Definitions:

Digitally Signed:

A digitally "signed" document usually displays a green check mark signature. Once a document has been signed, someone can modify the document, but if they do, the graphic on the signature changes (usually a red x) to indicate that the document has been modified since signing.

Digitally Certified:

Documents can also be "certified." This generally displays a blue ribbon signature. The person certifying the document can allow people to add signatures after the document is certified, but people can only change what the certifier allows. For example, one person might certify the document, but others add their signatures to sign off on various pages in the document.

Paragraph 4

(4) Alternatively, electronic files may be signed and sealed by creating a "signature" file that contains the surveyor and mapper's name and PSM number ***(Item 1***), a brief overall description of the surveying and mapping documents ***(Item 2)***, and a list of the electronic files to be sealed ***(Item 3).***

Each file in the list shall be identified by its file name utilizing relative Uniform Resource Locators (URL) syntax described in the Internet Architecture Board's Request for Comments

(RFC) 1738, December 1994, which is hereby adopted and incorporated by reference by the Board and can be obtained from the Internet Website: ftp://ftp.isi.edu/in-notes/rfc1738.txt. ***(Item 6)***

Each file shall have an authentication code defined as an SHA-1 message digest described in Federal Information Processing Standard Publication 180-1 “Secure Hash Standard,” 1995 April 17, which is hereby adopted and incorporated by reference by the Board and can be obtained from the Internet Website: http://www.itl.nist.gov/fipspubs/fip180-1.htm. ***(Item 4)***

A report shall be created that contains the surveyor and mapper’s name and PSM number, a brief overall description of the surveyor and mapper documents in question and the authentication code of the signature file. This report shall be printed and manually signed, dated, and sealed by the professional surveyor and mapper in responsible charge. ***(Item 5)*** The signature file is defined as sealed if its authentication code matches the authentication code on the printed, manually signed, dated and sealed report. Each electronic file listed in a sealed signature file is defined as sealed if the listed authentication code matches the file’s computed authentication code.

Rulemaking Authority 472.008, 472.025 FS. Law Implemented 472.025 FS. History–New 2-1-00, Amended 12-16-07, Formerly 61G17-7.0025.

General notes for both rules:

- *(Item 4)* SHA-1 calculation is done by Java API, which uses the FIPS PUB 180-1 as identified in paragraph four of 61G15-23.003.
- The District uses an independent SHA-1 testing application located at this link. http://www.karenware.com/powertools/pthasher.asp This application verifies that the calculated numbers are valid.
- Any edits made to files submitted to the District files are saved to copy. The original file is not changed and SHA-1 codes are verified by our staff as matching the signature document when it is received.
- Uniform Resource Locators (URL) syntax ***(Item 6)*** is not used since files are stored in our database and not referenced via this syntax.
- Examples can be seen at:
    - Digitally (PKI) signed plans [Very large file 18M]: https://permitting.sjrwmd.com/apps/idcplg?IdcService=GET_FILE&coreContentOnly=1&RevisionSelectionMethod=Latest&allowInterrupt=1&dDocName=EREG_2050865
    - Sign and Seal document for plans: https://permitting.sjrwmd.com/apps/idcplg?IdcService=GET_FILE&coreContentOnly=1&RevisionSelectionMethod=Latest&allowInterrupt=1&dDocName=EREG_2176330

Item 5

Division of Regulatory Information Management
P.O. Box 1429
Palatka, FL 32178-1429

SIGNATURE DOCUMENT

Permit Number: 96932 - 4
Submittal Confirmation Number: 204473
Project Name: Lost Tree Preserve (Transfer)

This document is signed and sealed to secure the electronic files referenced by the signature files as described in the Florida Department of Business and Professional Regulation.

Signature File Created: Tue Jan 11 11:12:15 EST 2011

Number Signed/Sealed Files: 2

Name: John Smith ← Item 1

Type of Professional Registration: PE

License Number: 12345

Signature: _____

Date: _____

Item 3 →

SIGNATURE FILE NAME: sha.png
SHA-1: DFB66219BF98A5BE4EB80475B8478BB0C8BDA723 ← Item 4
DESCRIPTION: Plans page 1 ← Item 2

SIGNATURE FILE NAME: afiedt.txt
SHA-1: 43BC9A29519CB27AB5D9538D20F0196F1E2451FF
DESCRIPTION: Calculations

-- End of Signature Document --

Item 6

E-Permitting account holders have been provided a tool to verify the file and associated SHA-1 number in our database match the submitted file on their local drive. Selecting the file on the local drive and clicking Verify highlights the matching filename/SHA-1 combination. If no matching SHA-1 number is found, a message is displayed indicating that no match was found.