CITY OF TALLAHASSEE **Administrative Policies and Procedures Manual**	**DATE** 1/1/2010
	NO. 407
TITLE CITY OF TALLAHASSEE POLICY ON ELECTRONIC DIGITAL SIGNATURE, ELECTRONIC SEALS AND ELECTRONIC NOTARY	**ORG. AGENCY** DMA/ISS
	APPROVED

407.01	STATEMENT OF POLICY Chapters 668, 117 and 471 of the Florida Statutes, Chapter 61G15-23 of the Florida Board of Engineers outline the requirements for the application and use of Electronic Digital Signatures as a means for Engineers to seal documents and the use of Electronic Notary.
407.02	AUTHORITY City Manager Directive
407.03	OBJECTIVE To establish a uniform procedure for the acceptance of the use of Electronic Digital Signatures as a means for an Engineer to seal documents and the use of Electronic Notary as a means for a Notary to notarize documents submitted to the City of Tallahassee as outlined under State law. This document sets forth the requirements and process for acquisition and use of electronic digital signatures through the use of Public Key Infrastructure (PKI) as the method of Electronic Digital Signature in regards to the application of "Electronic Notary" and "Electronic Seal" accepted by the City of Tallahassee.
407.04	SCOPE AND APPLICABILITY The use of these procedures outlined in this policy shall apply to all departments that require notarized or sealed electronic documents.
407.05	DEFINITIONS Elements of Electronic Digital Signatures, Electronic Seals and Electronic Notary include: 1. Public Key Infrastructure (PKI), a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. 2. Certificate Authority (CA) also known as Trusted Third Party (TTP), a third party who issues an Engineer or Notary their electronic credentials to engage in Electronic Digital Signature through the use of a Certificate.

3. Certificate, an electronic document that uses a digital signature to bind together a public key with an identity that:
    a. Identifies the certificate authority;
    b. Identifies the subscriber;
    c. Contains the subscriber's public key; and
    d. Is digitally signed by the certification authority.

4. Digital Signature, a type of electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the intial message and the signer's public key can accurately determine:
    a. Whether the transformation was created using the private key that corresponds to the signer's public key; and
    b. Whether the initial message has been altered since the transformation was made.

5. Electronic Seal, a unique digital signature used in conjunction with requirements of the Florida Board of Engineers that is used by an Engineer to authenticate electronic plans or renderings. Because the electronic seal is password protected, it is accessible only to its designated Engineer.

6. Electronic Notarization, also known as Electronic Notary Signature, a unique digital signature used in conjunction with requirements of the Chapter 117.021 Florida Statutes, and e-notarization rules promulgated by the Florida Department of State that is used by a Notary to authenticate an electronic notarial act. Because the electronic notarization is password protected, it is accessible only to its designated Notary.

7. Electronic Signature, any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with intent to authenticate a writing. A writing is electronically signed if an electronic signature is logically associated with such writing.

407.06 RESPONSIBILITIES

<u>Responsibilities of City Staff:</u>

Any City staff member who is responsible for the receipt or validation of electronically "Signed Documents," "Sealed Documents," or "Notarized Documents" shall:

1. First, verify that the "Electronic Digital Signature" is valid and unaltered by accessing the "Certificate" through the "Certificate" icon on the "Electronic Signature" and

2. Second, verify that the additional requirements for the "Electronic Digital Signature", as required by the governing board of the profession of the person whose "Electronic Digital Signature" appears on the electronic document, are present such as the P.E number of an Engineer or the Commission Expiration date of a Notary.

Responsibilities of Submitter:

Any person or agency 1) who chooses to submit electronic documents that include an "Electronic Digital Signature," when the receiving City agency allows for this type of submittal or 2) who is required to submit electronic documents to a City agency shall:

1. Have applied for and received their electronic credentials (Electronic Digital Signature) from a Certificate Authority (CA) also know as a Trusted Third Party (TTP) that issues these credentials according to the State of Florida guidelines of using Public Key Infrastructure (PKI);

2. Comply with any requirements of their professional governing board with regard to their "Electronic Signature," "Electronic Seal," or "Electronic Notarization"; and

3. Adhere to all other submittal requirements set forth by the City of Tallahassee for the particular document type in question.

407.07 PROCEDURES

To acquire and use an "Electronic Digital Signature" for the purpose of "Electronic Seal," or "Electronic Notary," the following steps should be taken:

1. Review the State of Florida's requirement for "Electronic Digital Signatures" as outlined in the Florida Statutes referenced in the Statement of Policy section of this document for Public Key Infrastructure (PKI);

2. Review the rules and regulations of the Governing Board of your profession or service for their acceptance and additional requirements for "Electronic Digital Signatures" in regards to "Electronic Seal," and "Electronic Notary," such as the Board of Engineers or Chapter 117.021 Florida Statutes, and e-notarization rules promulgated by the Florida Department of State as referenced in the Statement of Policy section of this document;

3. Locate a company who acts as a "Certificate Authority" that will issue an "Digital Signature" (Electronic credentials) based on Public Key Infrastructure (PKI);

4. Apply your "Electronic Digital Signature" as dictated by your "Certificate Authority." (CA)

407.08 EXCLUSIONS

This policy specifically excludes the "Secure Hash Standard" as described in the Federal Information Processing Standard Publication 180-3 (2008). This exclusion does not include "Secure Hash Standard" method from any hash mark processes used in the PKI process. The "Secure Hash Standard" is not in keeping with the intent of this policy that seeks to recognize the method of Electronic Signature, Electronic Seal and Electronic Notary through the use of a widely accepted and applicable technology delivered with a high ease of use.

407.09 EFFECTIVE DATE

This policy is effective as of January 1, 2010.