March 2001

EXECUTIVE OFFICE OF THE GOVERNOR
NOTARY SECTION
Notary E-Mail E-ducation March 2001

Greetings Florida Notaries!

Here is the final installment of our series on electronic notarization:

HOW DO E-NOTARIZATION AND E-SIGNATURES WORK?

How can a notary digitally sign a document? Typically an electronic version of a document (e.g., a Word or Excel document) or online form is presented to a notary public. The notary administers an oath or takes the acknowledgement of the document signer, remembering that all current notary law, (Florida Statutes, Chapter 117), must be followed. The document is then signed with a digital certificate or with a UCC signature (typing their name in a box). In turn, the notary also digitally signs the document in a similar fashion. The document is now electronically notarized and can be transmitted (e.g., via email) or saved to disk. The process is practically the same as that of paper notarization.

The actual process of digitally notarizing an electronic document can be implemented by a number of various structures and approaches that allow us to realize the benefits of e-transactions and e-notarizations. The underlying technology in accomplishing secure transactions and authenticating individuals is encryption. Encryption is a process that transforms data to an unreadable format so that the information remains secure. This allows for a measure of authenticity, integrity, and confidentiality. In short, by using this technology, one can validate the integrity of the document and verify the identity of an individual - the key to notarizing online documents.

Digital notarizations commonly use digital signatures, a type of electronic signature, in place of wet signatures. A digital signature, using the technology of a digital certificate, is a form of encrypted data that can be used to authenticate an individual and his or her document.

The technology that allows for digital certificates and electronic signatures is precisely what makes electronic notarization legally acceptable. A digital signature is part of a system called Public-key Infrastructure (PKI) and has a corresponding component called a digital certificate. PKI is the generally accepted method of ensuring e-commerce security. Confidentiality, authentication, integrity and non-repudiation are four important ingredients required for trust in e-commerce transactions. The emerging response to meet these requirements is the implementation of PKI technology. In basic terms, PKI allows an individual to obtain a digital certificate, which then would be used to affix that individual's digital signature to an electronic document. A digital certificate holds vital information and allows for authentication of the individual, through the use of two related "keys," your private key and your public key, known as a key pair.

Public key infrastructure incorporates various terms and technologies such as message digests (hash functions), asymmetric cryptography, tokens, X.509 certificates, public and private keys, nonrepudiation, and others. There is no doubt that the technologies used to digitally sign documents can be daunting. But for you, the notary, using this technology is completely transparent. Electronic notarization is achievable without requiring you to know the fundamental technology, allowing you to expand your notarial role without having to invest a lot of time in learning a new technology.

A digital certificate is a credential (think of it as a driver's license online), issued by a trusted third party, known as a Certification Authority, that validates individuals or organizations. A digital certificate is the foundation that allows a user to authenticate other users and to sign transactions with legally binding signatures.

The Certification Authority (CA) maintains digital certificates and serves to validate a digital signature (and therefore a notarization's signatory). As stated, various firms act in this capacity, including ARCANVS, Baltimore Technologies, Entrust Technologies, Thawte, and Verisign. Though methods and authentication procedures vary, all CA's provide a means to distribute digital certificates, maintain a repository of their issued certificates, and validate the identity of any certificate holder.

That is all there is to it! The procedure remains essentially the same. You can view a digital signature as another form of the traditional pen - one you use to sign the document.

HOW DO I BEGIN?

To begin with, you can start by learning more about digital certificates and electronic security measures such as PKI. Contact any certification authority that specializes in witnessed-identity authentication. Additionally, there are several online sites that offer a wealth of information concerning security in an electronic arena.

Second, research companies that offer digital certificates and become familiar with the electronic notarization environment. The need remains the same, but there are differences in how an electronic document is notarized. Knowing how the procedures work will ensure a smooth transition to electronic transactions, as well as make you an expert.

Finally, relax! Technology does not necessarily mean adverse change. Recognizing the benefits that electronic notarization provides will help you allay any concerns. Your role will not diminish. On the contrary, incorporating electronic notarization into your functions will prepare you for the future - and add skills that make you more valuable to your employer and clients.

Thank you for your time!
Jennifer Bertsch
Notary Education Coordinator
State of Florida, Office of the Governor
FL_GOV_NOTARY@EOG.STATE.FL.US