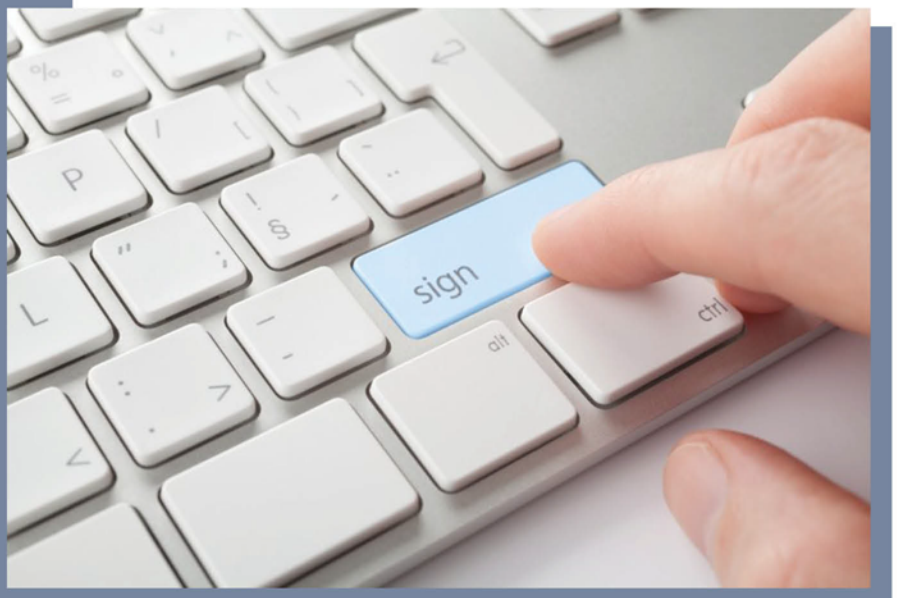
Notices and Offers by Electronic Methods: Process Streamlining



Literature and Web Research

Final Report
October 2015

Prepared for:
United States Department of Transportation
Office of Planning, Environment and Realty
Federal Highway Administration

U.S. Department of Transportation
Federal Highway Administration

Table of Contents

Preliminary Outline

- **I. Introduction – Overview of Research Study**
- **II. Background**
  - a. History of signed documents
  - b. Historical regulatory requirements
- **III. Major Legislation to Standardize Electronic Transactions and Signature Verification**
  - a. Types of transactions
    - i. Verbal/handshake
    - ii. Signed documentation
    - iii. Notarized documentation
    - iv. Electronic signature legislation
  - b. Uniform Electronic Transaction Act (UETA)
    - i. Rules of an electronic signature
    - ii. Overcoming identification and attribution obstacles
    - iii. Procedural act vs. substantial act
      1. Both parties must agree
      2. Nobody is forced
    - iv. Validation of electronic agents
    - v. States that have adopted UETA
  - c. Electronic Signatures in Global and National Commerce Act (ESIGN)
    - i. Federal Trade Commission role
    - ii. Basic provisions of ESIGN
- **IV. Electronic Signatures**
  - a. Validity and types of electronic signatures and digital signatures
  - b. Security considerations
    - i. Requirements
    - ii. Three security levels for legitimacy
    - iii. Use of cryptography and Public Key Infrastructure (PKI)
  - c. Examples of e-signatures
  - d. Documents that still require a paper signature
- **V. Electronic Signature Services**
  - a. Cloud based-services
  - b. Existing service providers
    - i. DocuSign
    - ii. Adobe EchoSign
    - iii. Sertifi
    - iv. RightSignature
    - v. Silanis
- **VI. Electronic Signature Studies and Use of Electronic/Digital Signatures by State DOTs**
  - a. Electronic Signature Pilot Project by Volpe National Transportation Center

DTFH61-11-D-00037-T-13002

Notices and Offers by Electronic Methods: Process Streamlining

Literature and Web Research

Introduction

This research study, *Notices and Offers by Electronic Methods: Process Streamlining*, will provide technical information related to the use of internet-based systems that can be used to streamline the right-of-way (ROW) acquisition process, including the relocation assistance process. This research will specifically examine whether these internet-based systems will assist in the delivery of various notices that are required under 49 CFR 24.102(b), which requires the Agency to notify the owner in writing, as soon as feasible, of its interest in acquiring the real property and the basic protections provided to the owner by law and the regulations. The research study will also investigate the use of these internet-based systems for the delivery of the written offer to acquire and summary statement required under 49 CFR 24.102(d) and (e), the explanation of the offer required under 49 CFR 24.102(f), and the required notices under 49 CFR 24.203, all of which are essential to the ROW process.

The delivery of notices is addressed in 49 CFR 24.5 – *Manner of notices*

Each notice which the Agency is required to provide to a property owner or occupant under this part, except the notice described at § 24.102(b), shall be personally served or sent by certified or registered first-class mail, return receipt requested, and documented in Agency files. Each notice shall be written in plain, understandable language. Persons who are unable to read and understand the notice must be provided with appropriate translation and counseling. Each notice shall indicate the name and telephone number of a person who may be contacted for answers to questions or other needed help.

In *Task 3 – Literature and Web Research*, a web-based search for relevant articles, case studies, and other legal doctrine addressing the use of electronic delivery and signature verification technology was performed, specifically in government uses. The following articles were researched for this report, and are listed in more detail in the attached bibliography.

- A Discussion About S-Signatures With Examples
- Adobe EchoSign Security Overview
- A Primer on E-Commerce Law in Florida
- Contracts and Electronic Signatures
- Digitally Encrypted Electronic Signatures
- Digital Signatures at LaDOTD
- DocuSign for Real Estate
- E-signatures: The complete guide to paperless signing
- Electronic Signatures and Online Contracts
- Electronic Signature

- Electronic Signatures in Global and National Commerce Act
- Electronic Signature Pilot Project by Volpe National Transportation System Center
- Electronic Transactions Act Summary
- Field Guide to Electronic Signatures
- How to Make Sure that Digital Signature is Legit
- S-Signature Examples, 37 CFR 1.4(d)(2) effective September 21, 2004
- Silanis: Government
- Silanis: Louisiana Department of Transportation & Development Chooses Silanis for Web-based Electronic Signing
- Terminology from the South Dakota State Legislature regarding Electronic Transactions
- Uniform Electronic Transactions Act – States who have adopted UETA

A summary of current industry leaders providing digital signature services was completed, as well as a general overview of how these services function, and may be adapted to a DOT or other agency to streamline the ROW acquisition process. The existing requirements for delivery of notices and offers under 49 CFR Part 24 currently represent a barrier to these streamlining efforts, however, research conducted as part of this task will assist the FHWA in determining whether state-of-the art electronic delivery or signature verification methods can be used to streamline or update current requirements. Research for subsequent tasks will identify when it is and is not appropriate to use electronic methods of transmittal for notices and making offers.

Background

The use of a personal signature has historically been utilized to authenticate a document. Although signatures are susceptible to forgery, throughout history the use of signatures are unique enough to represent a personal guarantee of individual approval. Dating back to the 1800's, common law jurisdictions accepted telegraph signatures and more recently, faxed signatures in the 1980's. With the rapid development of digital technology, it has become increasingly more common for documents to be communicated in electronic form. Because the act of verification of receipt and acceptance of electronic documents could be delayed by utilizing handwritten signatures, a variety of systems of electronic signature have been developed (see the section titled "Electronic Signatures" below). Further evolving are the methodologies of secure electronic and digital signatures.

Traditionally, the acceptance of terms and conditions of many types of transactions or arrangements could be considered legally binding by merely acknowledging a verbal acceptance or using a handshake. The more important arrangements, including most types of real property transfers, required a written form of documentation with signatures. Often times, these more important documents required some type of notarization of signature, or witness verification. Over time and generally through the application of case law at the state level, a

general consensus of the level of documentation necessary to validate various contracts and acceptances of terms developed.

Although the Uniform Act does not specifically address the method of delivery of notices, the implementing regulations at 49 CFR Part 24 have historically required personal delivery, or delivery by certified or first-class mail, return receipt requested. If personal delivery could not be accomplished, the certified or first-class mail was the most common form of delivery available. These forms of delivery also demonstrated proof of delivery for an Agency's file documentation.

Major Legislation to Standardize Electronic Transactions and Signature Verification

With the onset of electronic communication, and the ease of sending and receiving documents electronically, a new system of document verification became necessary. The two major pieces of legislation that were enacted to aid in the standardization of electronic transaction and signature verification were the Uniform Electronic Transaction Act (UETA) in 1999, and the Electronic Signatures in Global and National Commerce Act (ESIGN) in 2000. These two laws established the framework for adapting the digital and electronic age of communication to the existing standards of document acceptance and verification. For the most part, these laws are procedural with the ultimate goal of consumer protection. The various applications of electronic signatures are generally left open for organizations to choose which software or method of acceptance and delivery meet their needs.

Uniform Electronic Transaction Act (UETA)

This Act was promulgated under the direction of the National Conference of Commissioners on Uniform State Laws (NCCUSL) in 1999, with four basic rules:

1. A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
2. A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
3. Any law that requires a writing, will be satisfied by an electronic record.
4. Any signature requirement will be met if there is an electronic signature.

Since the traditional and statutory rules that govern mail delivery cannot be applied to electronic transactions, this Act has the effect of determining when information is legally delivered in electronic form. A date and timestamp establishes the date of delivery and receipt with an electronic record capable of retention.

Since electronic transactions are mostly faceless transactions between strangers, the UETA states that a signature is attributable to a person if it is an act of that person, and this act may be demonstrated in any manner. In the faceless environment of electronic transactions, the obvious difficulties of identification and attribution must somehow be overcome, and the UETA provides guidance on how identification can be most effective.

The UETA does not attempt to create a new system of legal rules regarding electronic transactions, but has the objective of assuring that transactions in the electronic marketplace are as enforceable as transactions memorialized on paper and with manual signatures. The UETA is technically neutral, as it does not place any requirements regarding how any security procedures should be utilized, and it is considered to be a procedural Act as opposed to a substantial Act. Nothing in the Act requires the use of a digital signature or any security procedure. UETA applies only to transactions in which each party has agreed by some means to conduct them electronically. Agreement is essential and no one is forced to use electronic signatures.

The UETA clearly validates contracts formed by electronic agents, which are defined as computer programs that are implemented by their principals to do business in electronic form. They operate automatically without human supervision, though they are certainly not autonomous agents, and are a tool that parties use to communicate. This means that the person or entity which provides the program to do business is bound by the contract that its agent makes.

As of this date, forty-seven States have officially adopted the provisions as contained in the UETA.

Electronic Signatures in Global and National Commerce Act (ESIGN)

This law was enacted in 2000 to facilitate the use of electronic records and signatures in interstate and foreign commerce, by ensuring the validity and legal effect of contracts entered into electronically. It placed the Federal Trade Commission (FTC) in the position of assuring that the risk of fraud does not outweigh the benefits of electronic commerce. Through a series of subsequent hearings and investigations, the FTC did, in fact, conclude that the provisions of ESIGN were being effectively implemented. The basic provisions of ESIGN include:

1. Information required by law to be in writing can be made available electronically to a consumer only if the consumer affirmatively consents to receive the information electronically, and the business discloses specified information to the consumer prior to receiving consent.
2. A consumer's consent to receive electronic records is valid only if it can be reasonably demonstrated that the consumer can access the information in the electronic form in which the information will be provided.
3. Certain existing state and federal laws requiring the delivery of written information can be complied with electronically, whether the information is a disclosure, a notice, or a statement of rights and obligations, within the context of a business to consumer transaction.

Electronic Signatures

Under the provisions of ESIGN, electronic signatures are just as valid and enforceable as those signed by a contracting person's own hand. An electronic signature (or e-signature) is an electric sound, symbol, or process attached to or logically associated with a record, and adopt by a person with the intent to sign the record. The most popular method for gathering and managing electronic signatures uses an individual's e-mail address to identify each participant and associate them with a sequence of events that demonstrates an intent to sign.

A digital signature is a specific type of electronic signature, which requires a signer to have a certificate-based digital identification. This digital identification is frequently contained in a token, a smart card, or other physical device. A digital signature is most frequently used in large governmental agencies and regulated industries for internal business-to-business workflows.

In order for an electronic signature to be considered secure, it must:

1. Be unique to the person making the signature.
2. Use technology or a process to make the signature under the sole control of the person making the signature.
3. Use technology where the process can be used to identify the person using the technology.
4. Use technology where the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed subsequent to when the electronic signature was applied to the document.

There are three security levels of legitimate e-signatures:

- Level 1 (low-level secure): Use of a picture of a signature such as a .jpg in a .DOC or .PDF file. This is not a recommended practice.
- Level 2 (mid-level secure): Use of S-signatures as follows:
    - /s/John Smith - Submissions to the Federal Court Systems
    - /John Smith/ - Submissions to the Patent & Trademark Office
      John Smith
- Level 3 (high-level secure): Use of services such as DocuSign, EchoSign, etc. which follow the letter and intent of the E-Sign Act. This should be the choice for all high-value transactions, such as real estate contracts.

One of the most secure methods of establishing electronic signatures is to use the science of cryptography, which provides a means of scrambling information from the sender and allowing the receiver to unscramble the information. There are a number of cryptographic methods, with one of the most popular being Public Key Infrastructure (PKI). This method meets the security Level 3 described above.

ESIGN does provide that prior to getting a consumer's consent for using electronic contracts and signatures, the consumer must be notified whether or not there are paper copies of the

documents that can be used as an alternative. The Act also provides that once a business receives consent for electronic delivery, the consumer can later change his/her mind and switch to paper documents. Because electronic signatures are not like paper, the consumer must be given notice regarding the hardware and software requirements necessary for formalizing the contact electronically.

The specific federal regulations which set out the format and examples for an electronic signature can be found at 37 CFR 1.4(d)(2), and have an effective date of September 21, 2004. These regulations fall under the purview of the United States Patent and Trademark Office, and give examples of what is considered to be proper signature format in a variety of signature situations.

There are still certain types of contracts and documents that are required to be on paper in order to protect consumers. These documents include:

- Wills, codicils, and testamentary trusts
- Documents relating to adoption, divorce, and other family law matters
- Court orders, notices, and other court documents such as pleadings or motions
- Notices of cancellation or termination of utility services
- Notices of foreclosure, eviction, repossession or default
- Notification of termination of health or life insurance benefits
- Notices of product recall affecting health or safety
- Documents that are required to travel with hazardous materials
- Documents that must be notarized
- Deeds and other real property transfer records

Electronic Signature Services

A variety of cloud-based services have been established to take advantage of e-signing, adding various features that may make that service more appropriate for any particular type of usage. Cloud-based applications live on the Internet rather than on a local computer (cloud is really just another word for the Internet). The major advantage for users is that they can access those applications wherever they are, as long as an Internet connection is available. The users can choose to store the documents associated with those applications in the cloud too, and can access the equivalent of their working desktop wherever they are.

The following existing and acknowledged service providers are all web-based, or cloud-based.

DocuSign is a major provider to the real estate industry, and the official and exclusive electronic signature provider to the National Association of REALTORS©. This service allows agents to manage the entire transaction online securely with all participants. The program includes document collaboration designed to accelerate real estate transactions, so the parties can store, manage and share documents all in one location. DocuSign provides Level 3 security, the highest level.

Adobe EchoSign is similar to DocuSign, with some unique aspects. This provider emphasizes data protection and security procedures, also providing Level 3 security. Users are typically

created by account administrators and must login with their email and password to gain access to the application. All data within the application is access controlled with a role-based model; the user must be a participant in the document, such as the sender or the signer, in order to view it or sign it. Customer account administrators can create, deactivate, and reactivate users in their accounts, create groups and move users between groups.

Sertifi is more basic than other providers. It focuses on providing its customers the ability to get sales agreements signed faster by automating the execution of contracts or agreements. It allows users to send, manage, and track agreements, as well as retrieve and report on signed agreements/signing events. Sertifi offers Level 3 security.

RightSignature is also a more basic provider, however, it offers navigation for the signer, pointing to locations where they need to fill in information, initial, or sign. This provider also allows for sequential signing in the event documents must be executed by one party before another. Every executed document includes a RightSignature Certificate with court-admissable validity data, including an audit log and each party's name, email, signature, IP address, and other identity information. This service provides Level 3 security.

Silanis markets itself as a government provider, and is currently being employed by both the Kansas and Louisiana Departments of Transportation (see section titled "Electronic Signature Studies and Use of Electronic/Digital Signatures by State DOTs" below). Other government agencies use this service for e-contracting, task orders, procurement contracts, licensing and permits for citizens and businesses, recruiting and on-boarding of personnel of employees, and human resource and personnel forms. This service cuts costs by going paperless and improves responsiveness to the public. Silanis offers the highest level of security, a Level 3.

The cost of each of these services is dependent on several factors, such as the type of license an Agency seeks and the number of users it estimates. This research study will include examinations of several different electronic delivery or signature verification methods that may be used to expedite or streamline ROW acquisition. An identification of the costs to develop, deploy, use and support an electronic delivery or signature verification method for a State DOT will also be developed.

Electronic Signature Studies and Use of Electronic/Digital Signatures by State DOTs

Electronic Signature Pilot Project by Volpe National Transportation System Center

In 2007, the Volpe National Transportation Systems Center Planning Collaboration Initiative issued findings from their Electronic Signature Pilot Project. The purpose of the pilot project began in the Spring of 2005 with three goals: to better serve customers, to improve internal processes, and to reduce the time and expenses associated with the handwritten signature process. Because the project took place almost 8 years ago, the use of digital-based signatures were still evolving. The project required that the document must be compatible with Microsoft Word and Adobe Acrobat, and that it create and display a graphic signature image. The pilot project produced some key lessons learned through the process.

1. Institutional issues were more complex than technology

2. Face-to-Face training on the use of electronic signatures is better than simply providing written procedures
3. Forgetting passwords and losing files are potential challenges with electronically signed files.

This report provided the best definitions and differences between electronic signatures and digital signatures.

> **Electronic Signature**: A digital mechanism for identifying the signer or sender of an electronic document. This term most commonly refers to a digital illustration of a person's handwritten signature, inserted as a graphic element to mimic a hand-signed document. It can also refer to email headers and facsimile origination numbers. They do not provide proof that the person represented has actually "signed" the document or that the document hasn't changed since the signature was inserted.
>
> **Digital Signature**: An electronic and tamperproof seal that can be used to authenticate the identity of the person who "signed" a document or to indicate that the document has not been changed since the signature was added. All digital signature systems use some type of cryptography to prevent falsification of signatures.

Digital Signatures at the Louisiana Department of Transportation and Development (LADOTD)

In 2008, the Louisiana Department of Transportation began using the Silanis ApproveIt Signature Verification software to electronically process residential permit applications for driveways and mailboxes, using secure e-signatures. It had begun using Silanis' electronic signature technology two years earlier to streamline the internal approval process for engineering projects.

The signature verification has public information that includes a secure image of the person's handwritten signature, user profile, digital certificate and a unique public key. There is also a private portion that contains information only known to the signer, such as a unique, private password and private key. This information sets up the user's "ePersona," which can only be accessed upon entering the private password.

In 2009, the LADOTD expanded the use of the Silanis digital signature to the approval of plans. According to a report published the same year, the goal was to move to digital publishing, using a PDF input/output format. This would allow the drawings to be exported to a signature directory, and the engineer would sign them using Silanis ApproveIt. The "import" would check to make sure the drawings are signed, and execute them to set the plans to "final status."

The program would then set the signature status attribute to "signed." There would be a recorded audit trail of the signing ceremony. The plans could then be published to a PDF format.

Digitally Encrypted Electronic Signatures – Michigan Department of Transportation (MDOT)

In February, 2012 the Chief Operations Officer and Bureau Director of Field Operations for the Michigan Department of Transportation issued a Bureau of Highway Instructional Memorandum to MDOT's Region Engineers, Region Associate Operations Engineers, TSC Managers, and TSC Construction Engineers advising them that the Michigan Attorney General's Office, in concurrence with the Federal Highway Administration, had issued a decision authorizing MDOT to use and accept digitally encrypted electronic signatures. This Instructional Memorandum stated that digital electronic signatures would now be accepted wherever a signature is required on an MDOT. Although the Michigan Attorney General's decision did not limit the type of documents where a digital electronic signature could be used, it did require that the new use of documents or processes had to be first cleared with the Attorney General's office.

This Memorandum encourages the use of electronic signatures, stating it "can lead to significant monetary, resource, and time savings for all involved. New forms, innovative ideas, and process improvements are encouraged to be submitted for approval." The Memorandum provides additional information about MDOT policies for digital electronic signatures, and an attachment of instructions for users.

Barriers to the Use of Electronic Confirmation and Verification during the ROW Process

The primary barrier to using electronic delivery systems for relocation notices and written offers to acquire are the current Uniform Act implementing regulations at 49 CFR Part 24 that do not allow for such a delivery method. Some individual State laws may also prohibit the use of electronic delivery for written offers or certain notices, however, this is not viewed as an obstacle to any regulatory change that may occur. If a regulatory change did allow for the electronic delivery of written offers of notices, it would likely be in addition to personal delivery and mail delivery. Other barriers to using electronic delivery and signature verification may be the owner/displacee's lack of access to the information in an electronic form or an unwillingness to receive it in that form. Certain documents that are essential to the conveyance of the real property interest, either through a deed or the courts, cannot be signed electronically.

Summary/Recommendations

The information obtained during the literature review indicates that electronic delivery and signature verification systems can be incorporated into the ROW process. First, there are federal laws governing electronic signatures that set out the parameters for their use. The Uniform Electronic Transaction Act (UETA) established that an electronic record or signature

has the same force and effect as paper transactions with manual signatures. The use of electronic methods must be by mutual agreement, rather than mandatory. The Electronic Signatures in Global and National Commerce Act (ESIGN) ensured the validity and legal effect of contracts entered into electronically, however, the consumer has to consent to the electronic transaction. These laws provide the legal basis for incorporating electronic delivery and signature verification systems into several aspects of the process, such as delivery of notices, correspondences, written offers to acquire, and purchase contracts if the acquiring Agency follows the requirements described in the above sections, i.e., obtaining the consent of the owner/displacee to receive the documents electronically and providing the proper disclosures.

Second, there are electronic signature services available that can provide the necessary level of security to validate the identity of the person signing the electronic document by using an encrypted digital signature. Third, the information cited in the above section titled "Electronic Signature Studies and Use of Electronic/Digital Signatures by State DOTs" demonstrate that electronic delivery and signature verification systems can be adapted for use by State DOTs. The LADOTD in particular successfully used signature verification software to process permit applications from individuals outside the Agency, as a State DOT Right of Way office would need to do with property owners and displaced persons.

The FHWA can use the information collected in this literature and web research to establish the initial guidelines for using electronic delivery and signature verification systems in the ROW process as it performs a review of potential changes to 49 CFR Part 24. These initial guidelines could specify the legal requirements under the federal laws previously cited, as well as requiring an encrypted digital signature to validate the identity of the person signing any required documents.

It seems likely that electronic delivery and signature verification systems can be used in some aspects of the ROW process to provide better service to property owners and displaced persons, improve the internal process, and reduce the time and expense of obtaining handwritten signatures. It is also probable that this technology will not be suitable "across the board." The research necessary to determine the most appropriate use of this technology in the ROW process will be performed in the next task of this research study. As stated previously, it will be important to identify when it is and is not appropriate to use electronic methods of transmittal for notices and making offers.

It is difficult to determine whether any particular State DOT would be in a better position to employ their currently used electronic signature system for right-of-way related activities, or whether it would be advantageous to employ a commercially available system. For those States that already have an advanced internally developed system, expansion of that system for right-of-way may be the most cost effective. For States that are not as electronically advanced, the employment of an established electronic transmission service may be most advantageous.

There is a continuous and unstoppable trend towards utilizing electronic capabilities to manage document production and maintenance. Considering the availability of existing commercial services, it would seem logical that there would be considerable competitive interest in securing a modified service to accommodate State right-of-way needs regarding electronic document

maintenance and delivery. As in many applications, economies of scale could come into play, and it could be advantageous for a group of States to combine their interests in acquiring software to aid in the effort to establish a common electronic methodology to communicate with impacted property owners.

Bibliography of Reference Materials

Literature and Web Research

A Discussion About S-Signatures With Examples

Author Unknown, *A Discussion About S-Signatures With Examples.* Patentably Defined. The Law Office of Michael E. Kondoudis. March 31, 2010. Retrieved on October 17, 2013. *http://patentably defined.com/2010/03/31/a-discussion-about-s-signatures-with-examples/*

S-signatures have been used by the U.S. Patent Office for several years according to this article. An S-signature is an e-signed document whereas the signee's name is written after forward slashes (/).

Example: /John T. Smith/
John T. Smith

This is listed as a second level of security method according to the included article, *How to Make Sure that Digital Signature is Legit.* Examples are listed in the article.

Key Terminology:

S-Signatures: an electronic signature between forward slashes and includes any signature made by non-handwritten means (i.e., electronic or mechanical)

Adobe EchoSign Security Overview

https://www.echosign.adobe.com/en/home.html. Retrieved October 21, 2013.

Adobe EchoSign is one vendor of e-signature software that provides a secure system for safe digital transactions. This particular document provides an overview of the software's procedures in order to assure the client of its security and reliability.

A Primer on E-Commerce Law in Florida

Green, David A., Esq., Fox Rothschild LLP, *A Primer on E-Commerce Law in Florida,* South Florida Chapter FOCUS Newsletter 2Q12, pg. 4. Retrieved on October 17, 2013. *http://www.foxrothschild.com/newspubs/newspubsArticle.aspx?id=15032386693*

This article outlines Florida's electronic commerce statutes. It also indicates that the "S signature" on a document does not constitute as an electronic signature which is contradictory, however, to the two articles (*A Discussion About S-Signatures With Examples and S-Signature Examples, 37 CFR 1.4(d)(2) effective September 21, 2004*) listed in this summary of reference materials.

Key Terminology:

Electronic Signature: any letters, characters or symbols manifested by electronic or similar means

Contracts and Electronic Signatures

Author Unknown. *Contracts and Electronic Signatures.* FindLaw.com. Retrieved on October 17, 2013. *http://smallbusiness.findlaw.com/business-operations/contracts-and-electronic-signatures.html*

This article represents an overall summary of e-signatures and contracts including information on Cryptography (scrambling information from the sender and allowing the receiver to unscramble it). It also includes syntax data for programmers. Finally, it includes a list of documents that cannot be done electronically. This list is consistent with other articles found in this summary.

Key Terminology:

Electronic Contract: a document that is created, transmitted and signed, all in electronic form.

Cryptography: the means of scrambling information from the sender and allowing the receiver to unscramble it. *Example: Public Key Infrastructure (PKI).*

Digitally Encrypted Electronic Signatures

Johnson, Gregory C. and Van Portfliet, Randy R., Michigan Department of Transportation. (February 28, 2012) *Office Memorandum: Digitally Encrypted Electronic Signatures.* Retrieved October 21, 2013.

http://www.michigan.gov/documents/mdot/MDOT_IM12-02_378056_7.pdf

This Office Memorandum issued by the Michigan Department of Transportation outlines the use of Digitally Encrypted Electronic Signatures. It outlines the validation process to assure the signature is considered valid. One interesting aspect of this memo is the utilization of digital electronic signatures for any document that requires multiple signatures (such as contract revisions). Finally, it includes instructions for signing e-documents in Adobe Acrobat, Signature Validation, and Setting up New Digital Electronic Signature for the First Time.

Key Terminology:

Document Certification: allows the document creator to ensure that no changes will be made to the document after signing. If any changes are made to a certified document after a certifying signature they will be very apparent and prevent anyone else from validating said document. The option of document certification should only be used when there is only going to a single signature on a form or document.

Signature Validation: verification by the recipient of an electronically signed document to confirm the identity of the signer/sender before the electronic signature may be considered valid. The first (and typical) method is verification of the identity of the signer. If the was supposed to be signed by a certain person and their name appears, then this requirement has been met. Secondly, it is common to identify the method/source of delivery. If the document arrives from the signer's unique email address then the second validation method criterion has also been met.

Digital Signatures at LaDOTD

Ward, Hollis. (September 28, 2009). *Digital Signatures at LaDOTD.* 2009 IHEEP Conference. Retrieved on October 21, 2013.
http://www.dot.state.tx.us/iheep2009/presentations/0G3_Digital_Signatures_Panel_LaDOTD_HollisWard.pdf

This presentation delivered at the 2009 IHEEP Conference in San Antonio, Texas on September 28, 2009 by Hollis Ward, DOTD Design Automation Manager. The Louisiana Department of Transportation uses the Silanis ApproveIt Signature Verification software to approve plans and outlines the process for retrieving e-signatures.

Key Terminology:

Digital Signature: an electronic authentication process attached to or logically associated with an electronic document. The digital signature must be:

i. unique to the person using it
ii. capable of verification
iii. under the sole control of the person using it
iv. linked to a document in such a manner that the digital signature is invalidated if any data in the document is changed

DocuSign for Real Estate

http://www.docusign.com/solutions/industries/real-estate. Retrieved on October 21, 2013.

DocuSign is another e-signature provider. This document outlines the benefits of e-signature in the real estate world. They are the "official and exclusive electronic signature provider to the National Association of REALTORS®, under the REALTOR Benefits® Program.

E-signatures: The complete guide to paperless signing

Null, Christopher (April 26, 2013). *E-signatures: The Complete guide to paperless signing.* PC World Magazine. Retrieved on: October 21, 2013. *http://www.pcworld.com/article/2035744/e-signatures-the-complete-guide-to-paperless-signing.html*

This guide to electronic signatures from PC World Magazine discusses the legality of e-signed contracts and includes a link to ESIGN Act which gives e-signatures the same legal weight as manual signatures. The article also includes their version of the most popular vendors of e-signature options to include DocuSign, Adobe EchoSign, Sertifi, and Right Signature. Silanis is not listed in this particular article.

Electronic Signatures and Online Contracts

Author Unknown. *Electronic Signatures and Online Contracts.* NOLO.com. Retrieved on October 17, 2013. *http://www.nolo.com/legal-encyclopedia/electronic-signatures-online-contracts-29495.html*

The information included in this article includes the basics of e-signatures to the types of signatures obtained through the process. These include Cryptographic Signatures (PKI) which scramble and unscramble data. This Public Key Infrastructure is believed to be the most secure and reliable method of signing contracts online. It also outlines XML-Based signatures which offer a method of a digitally-recorded fingerprint and hardware that electronically records a signature. This article also includes a list of documents that must be on paper and the site includes a two-minute video on how to make an electronic agreement.

Key Terminology:

Electronic Contract: an agreement created and "signed" in electronic form – in other words, no paper or other hard copies used.

Cryptography: the science of securing information.

Electronic Signatures in Global and National Commerce Act

Federal Trade Commission. (June 27, 2001). *Electronic Signatures in Global and National Commerce Act*. Retrieved on October 17, 2013. *http://www.ftc.gov/os/2001/06/esign7.htm*

This article provides information regarding "interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically." It discusses benefits to the consumer as well as the merchant and includes a list of benefits and burdens of e-signatures.

Key Terminology:

Electronic Signatures in Global and National Commerce Act (ESIGN): An act that went effective in October 2000, outlining the use of electronic records and contracts entered into electronically.

Electronic Signature Pilot Project by Volpe National Transportation System Center

Volpe National Transportation Systems. *Electronic Signature Pilot Project.* (2007)

In 2007, the Volpe National Transportation Systems Center Planning Collaboration Initiative issued findings from their Electronic Signature Pilot Project. The purpose of the pilot project was to better serve customers, to improve internal processes, and to reduce the time and expenses associated with the handwritten signature process.

Key Terminology:

Electronic Signature: A digital mechanism for identifying the signer or sender of an electronic document. This term most commonly refers to a digital illustration of a person's handwritten signature, inserted as a graphic element to mimic a hand-signed document. It can also refer to email headers and facsimile origination numbers. They do not provide proof that the person represented has actually "signed" the document or that the document hasn't changed since the signature was inserted.

Digital Signature: An electronic and tamperproof seal that can be used to authenticate the identity of the person who "signed" a document or to indicate that the document has not been changed since the signature was added. All digital signature systems use some type of cryptography to prevent falsification of signatures.

Electronic Transactions Act Summary

Uniform Law Commission. *Electronic Transactions Act Summary.* Retrieved on October 16, 2013. *http://uniformlaws.org/ActSummary.aspx?title=Electronic Transactions Act*

The Uniform Electronic Transactions Act (UETA) is included with this summary. The summary discusses the enactment of UETA in 1999 and outlines the basic rules governing the act. UETA's objective is to assure that an electronic signature (record) is given the same legal equivalency as a paper record with a manual signature.

Key Terminology:

Uniform Electronic Transactions Act (UETA): the first comprehensive effort to prepare state law for the electronic commerce era.

Transaction: an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Electronic Commerce: persons doing business with other persons with computers and telephones or television cable lines.

Electronic Agents: computer programs that are implemented by their principals to do business in electronic form.

Field Guide to Electronic Signatures

National Association of Realtors Library. (December 2012). *Field Guide to Electronic Signatures.* Retrieved on October 21, 2013.

http://www.realtor.org/field-guides/field-guide-to-electronic-signatures

This National Association of Realtors web page provides various links regarding the use of electronic signatures in real estate including the impact of e-signatures over a 10-year period, legal aspects and more. The National Association of Realtors uses DocuSign Electronic Signature Service to accelerate real estate transactions. This article also provides links to organizations and their usage of e-signatures, such as Bank of America, Fannie Mae, and Freddie Mac.

How to Make Sure that Digital Signature is Legit

West, Angela. (April 11, 2012). *How to Make Sure that Digital Signature is Legit.* Business and Finance Software; PC World Magazine. Retrieved on October 21, 2013.
http://www.pcworld.com/article/253523/
how_to_make_sure_that_digital_signature_is_legit.html

This article, also out of PC World Magazine, discusses ways to certify that e-signed documents will stand up in court. One method mentioned is to include several check boxes throughout a contract or document acknowledging the terms of the agreement. The article says, "A user who checks those boxes will have a hard time arguing later that they didn't understand what they were signing." It also lists the three security levels of e-signing and when not to use an e-signature.

S-Signature Examples, 37 CFR 1.4(d)(2) effective September 21, 2004

http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/sigexamples_alt_text.pdf

U.S. Patent Office. (October 27, 2004). *S-Signature Examples.* Retrieved October 17, 2013.

Another publication of the U.S. Patent Office, this lists proper and improper usages of an S-signature.

Silanis: Government

http://www.silanis.com/industries/government. Retrieved on October 21, 2013.

Silanis is an e-signature provider with many government contracts including the U.S. Army, U.S Air Force, U.S. Navy, U.S. Joint Chiefs of Staff, and the U.S. Treasury. More applicable to Task 3, Kansas Department of Transportation and the Louisiana Department of Transportation both use Silanis for their e-signature needs. The article also provides a list of transactions for government entities including, but not limited to, e-Contracting, procurement contracts, and licensing and permits for citizens and business.

Silanis: Louisiana Department of Transportation & Development Chooses Silanis for Web-based Electronic Signing

Silanis. *Louisiana Department of Transportation & Development Chooses Silanis for Web-based Electronic Signing.* News Releases. Silanis. Retrieved October 21, 2013. *http://www.silanis.com/about-us /news/louisiana-department-of-transportation-development-chooses-silanis-for-web-based-electronic-signing*

This news release from June, 2008, announces that Silanis has secured a contract to provide e-signature solutions to the Louisiana Department of Transportation.

Terminology from the South Dakota State Legislature regarding Electronic Transactions

South Dakota State Legislature. *53-12-1 Definition of Terms.* Accessed October 16, 2013. *http://legis.state.sd.us/statutes/PrinterStatute.aspx?Type=Statute&Statute=53-12-1*

> **Key Terminology:**
> Agreement: the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules and procedures given the effect of agreements under laws otherwise applicable to a particular transaction
> Automated transaction: a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract,

performing under an existing contract, or fulfilling an obligation required by the transaction

Computer program: a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result
Contract: the total legal obligation resulting from the parties' agreement as affected by

this chapter and other applicable law
Electronic: any technology using electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities
Electronic agent: a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual
Electronic record: a record created, generated, sent, communicated, received, or stored by electronic means
Electronic signature: an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record
Governmental agency: an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a state or of a county, municipality, or other political subdivision of a state
Information: data, text, images, sounds, codes, computer programs, software, databases, or the like
Information processing system: an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information
Person: an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity
Record: information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form
Security procedure: a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures
State: a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan native village,

which is recognized by federal law or formally acknowledged by a state
Transaction: an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs

Uniform Electronic Transactions Act – States who have adopted UETA

National Conference of State Legislatures. *Uniform Electronic Transactions Act.* Retrieved on October 17, 2013. *http://www.ncsl.org/research/telecommunications-and-information-technology/uniform-electronic-transactions-acts.aspx*

Information included in this article provides a map of the states who have adopted the UETA as well as a list of the year enacted and links to each state's statutory citation.

Glossary

Agreement: the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules and procedures given the effect of agreements under laws otherwise applicable to a particular transaction

Automated transaction: a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction

Computer program: a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result

Contract: the total legal obligation resulting from the parties' agreement as affected by this chapter and other applicable law

Cryptography: the science of securing and scrambling information from the sender and allowing the receiver to unscramble it. *Example: Public Key Infrastructure (PKI)*

Digital Signature: an electronic authentication process attached to or logically associated with an electronic document. The digital signature must be:

i. unique to the person using it
ii. capable of verification
iii. under the sole control of the person using it
iv. linked to a document in such a manner that the digital signature is invalidated if any data in the document is changed

Document Certification: allows the document creator to ensure that no changes will be made to the document after signing. If any changes are made to a certified document after a certifying signature they will be very apparent and prevent anyone else from validating said document. The option of document certification should only be used when there is only going to a single signature on a form or document.

Electronic: relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

Electronic agent: a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.

Electronic Commerce: persons doing business with other persons with computers and telephones or television cable lines.

Electronic Contract: an agreement created and "signed" in electronic form – in other words, no paper or other hard copies used.

Electronic Record: a contract or other record created, generated, sent, communicated, received, or stored by electronic means.

Electronic Signature: an electronic sound, character, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record, or associated with an electronic document

Electronic Signatures in Global and National Commerce Act (ESIGN): An act that went effective in October 2000, outlining the use of electronic records and contracts entered into electronically.

Governmental agency: an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a state or of a county, municipality, or other political subdivision of a state

Information: data, text, images, sounds, codes, computer programs, software, databases, or the like

Information processing system: an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information

Person: an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity

Record: information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form

Security procedure: a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures

S-Signatures: an electronic signature between forward slashes and includes any signature made by non-handwritten means (i.e., electronic or mechanical)

Signature Validation: verification by the recipient of an electronically signed document to confirm the identity of the signer/sender before the electronic signature may be considered valid. The first (and typical) method is verification of the identity of the signer. If the was supposed to be signed by a certain person and their name appears, then this requirement has been met. Secondly, it is common to identify the method/source of delivery. If the document arrives from the signer's unique email address then the second validation method criterion has also been met.

State: a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan native village, which is recognized by federal law or formally acknowledged by a state

Transaction: an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Uniform Electronic Transactions Act (UETA): the first comprehensive effort to prepare state law for the electronic commerce era

Notices and Offers by Electronic Methods: Process Streamlining
State Laws Addressing Validity of Electronic Signature

Each of the eight (8) State DOTs that were surveyed/interviewed in conjunction with the FHWA Research Study *Notices and Offers by Electronic Methods: Process Streamlining* has individual State laws governing the use of electronic documents and electronic signatures. Each of the State laws references compliance with the Uniform Electronic Transaction Act (UETA), and then goes on to codify such compliance within a Section of the State Code. Each State law lists compliance with the four basic rules of the UETA, which are:

1. A record or signature may not be denied legal effect or enforceability solely because it is in electronic form;
2. A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation;
3. Any law that requires a writing, will be satisfied by an electronic record; and
4. Any signature requirement will be met if there is an electronic signature.

Under the UETA and other federal regulations, including 37 CFR 1.4(d)(2), it is stated that, by law, certain types of contracts and documents may be determined to require a written signature, as opposed to an electronic signature. These exceptions may include documents such as:

1. Wills, codicils, and testamentary trusts.
2. Documents relating to adoption, divorce, and other family matters.
3. Court orders, notices, and other court documents such as pleadings and motions.
4. Notices of cancellation or termination of utility services.
5. Notices of foreclosure, eviction, repossession or default.
6. Notification of termination of health or life insurance benefits.
7. Notice of product recall affecting health or safety.
8. Documents that are required to travel with hazardous materials.
9. Documents that must be notarized.
10. Deeds and other property records.

A review of the laws of each of the eight (8) selected States indicates that none have laws which are stricter than the requirements of the UETA. With regard to exceptions to the legitimacy of electronic signatures, below is a summary of the State laws and how they relate to the ten (10) exception items as listed above.

State	Statute	Remarks
Indiana	Ind. Code §26-2-8-101 *et. seq.*	Electronic signatures are valid with the exception of (1) wills, codicils, and testamentary trusts, and (2) specific government exclusions. Specifically states that Electronic Notarization Signatures are acceptable.
Louisiana	La. Rev. Stat. §9.2601 *et. seq.*	Electronic signatures are valid with mostly the same exceptions as (1) the ten items as listed in UETA, and (2) banking documents as set out in the Uniform Commercial Code. Specifically states that Electronic Notarization Signatures are acceptable.
Michigan	Mich. Comp. Laws §450.831 *et. seq.*	Specifically states that Electronic Notarization Signatures are acceptable.
Mississippi	Miss. Code §75-12-1 *et. seq.*	Electronic signatures are valid with mostly the same exceptions as (1) the ten items as listed in UETA, and (2) banking documents as set out in the Uniform Commercial Code. Specifically states that Electronic Notarization Signatures are acceptable.

South Dakota	S.D. Codified Laws §53-12–1 *et. seq.*	Electronic signatures are valid with the exception of (1) wills, codicils, and testamentary trusts, (2) banking documents as set out in the Uniform Banking Code, and (3) transactions involving the Unified Judicial System. Specifically states that Electronic Notarization Signatures are acceptable.
Texas	Texas Business and Commerce Code §322.01 *et. seq.*	Electronic signatures are valid with the exception of (1) wills, codicils, and testamentary trusts, and (2) banking documents as set out in the Uniform Banking Code. Specifically states that Electronic Notarization Signatures are acceptable.
Utah	Utah Code §46-4-101 *et. seq.*	Electronic signatures are valid with the exception of (1) wills, codicils, and testamentary trusts, and (2) banking documents as set out in the Uniform Commercial Code. Specifically states that Electronic Notarization Signatures are acceptable.
Virginia	Va. Code 59.1 – 479 *et. seq.*	Electronic signatures are valid with the exception of (1) wills, codicils, and testamentary trusts, and (2) banking documents as set out in the Uniform Commercial Code.

SUMMARY

1. None of the State laws are more restrictive than the provisions of the UETA, and therefore would not likely prohibit the use of electronic document delivery and signature by the State DOT's

2. Six (6) of the eight (8) State laws only specifically exclude electronic signatures usage on documents defined as wills, codicils and testamentary trusts. Two (2) State laws expand the exclusion to many of the ten items listed as possible exclusions in the UETA (as set out above).
3. Seven (7) of the eight (8) State laws specifically allow the use of electronic signatures for notarization purposes, and the other State law does not prohibit such use.
4. Seven (7) of the eight (8) State laws specifically exclude the use of electronic signatures on items as set out in the Uniform Banking (Commercial) Code. This Code includes items such as funds transfers, warehouse receipts, investment securities, secured transactions, negotiable instruments, etc.