DocuSign

The fastest way to get a signature.®

WHITE PAPER

Detailed Discussion of the Legal Issues Surrounding E-Signature Deployment

Introduction

This document is part of a series provided by DocuSign, Inc. focusing on the delivery of business-class electronic signature services. This whitepaper discusses the legal issues that must be addressed in the deployment of e-signature services. It is not intended to replace a specific review of legal issues surrounding contract execution in any particular industry.

For additional information on other important issues, please refer to the companion whitepapers on:

- ***The Business Case for DocuSign***
- ***Security and Technology Advantages of the DocuSign Architecture***
- ***Legal Issues Whitepaper***

The following sections provide an overview covering 1) the evolution of electronic contracting, 2) the legislation enabling electronic signature usage and 3) the key legal factors for successful deployment of an e-signature system. Subsequent sections then provide detail regarding the specific ways that the DocuSignTM architecture addresses these critical legal issues.

What is an electronic contract?

It may be helpful to first make one point perfectly clear: under U.S. law (and under the law of most countries worldwide, although we won't attempt a detailed international analysis here) it is absolutely possible to form a contract electronically. E-SIGN and UETA have helped cement this conclusion, but really this wasn't a hard question even before these enactments.

Electronic contracting is, fundamentally, contracting and contract law fundamentals apply. Any contract, electronic or not, requires:

(a) "Offer,"
(b) "Acceptance", and
(c) "Consideration" – some promised exchange of value.
(d) "No defenses" - A contract, electronic or not, will not be enforced if a successful defense can be raised: for example, if an element of the contract is "unconscionable" (violates public policy), if one of the contracting parties was too young to create a contract, etc.

For the record, many U.S. courts have enforced electronic contracts, including 'click-wrap', and even recorded telephone agreements. (See Case Law section)

All this being said, there are two areas where electronic contracting raises some unique issues: (1) <u>"signed writing"</u> requirements, and (2) <u>proof</u> – i.e., proving contract formation, proving what the substantive terms of a contract are, and proving party identity. These are elements of contracting that have nothing to do with the signature itself, but deal with the process of signing an agreement.

In addition, many states have adopted another body of legislation called UETA (Uniform Electronic Transactions

Act), which strives to make interstate commerce smooth on a national level. These federal initiatives are intended to bring a common understanding to electronic commerce, and have provisions that can pre-empt state laws which are not consistent with them. In addition, this legislation has pre-empted inconsistent State laws that were technology centric around PKI-specific 'digital signature' requirements. As of May 2004, every state has legislation pertaining to electronic signatures. Most have adopted the Federal UETA process, while others have adopted similar laws.

E-SIGN broadly defines Electronic Signatures as *"an electronic sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."* This drafting was intentional to allow many types of technology (E-SIGN is technology neutral) and methods for signing electronically, while maintaining legal compliance. By definition then, *an electronic signature can be just about anything produced by electronic means (e.g., a symbol, result, or consequence), which has been created electronically in order to demonstrate a party's intent to sign an electronic record.* Specific examples of electronic signing include, entering a password or personal information number (PIN), typing a name where indicated (or prompted) via computer keypad, responding to telephone keypad agreements (e.g., "press 3 to agree or 5 to hear this menu again"), responding to click agreements, even responding to an email thread can constitute a digital signature.

It is important to keep in mind that legal digital signatures can take many different forms, ranging from smart cards and complex digital certificates to simple email responses. However, considering the realities and risks of the business world, it is important to implement E-SIGN provisions using a system that can provide auditable proof of the signature process and which can ensure non-repudiation to prevent legal challenges of the digital signature.

Key Factors for Enforceable E-Signatures

Intent

Intent is an important aspect of the e-signature process because it provides the legal "context" for enforceability. If the signer could claim to have "not understood" that they were actually signing a document, they might be able to mount a successful legal defense. With electronic signatures, the ability to establish intent can be of particular importance and can pose special challenges because the signing process does not take place within a structured physical setting (e.g. in a face-to-face meeting). Therefore the e-signature process should always provide a "structured online setting" that takes the signer through a series of steps, which make it clear that they are signing a legal document and confirms intent through overt actions, such as creating their signature and applying it to specific locations in the document.

Proof of Identity

Establishing the identity of the parties to the contract is a critical aspect of the signature process. In an online setting, this can be especially challenging because the parties do not "see each other" during the signing process and there is the risk that someone other than the intended signer(s) could be on the other end of the electronic transaction. Therefore, the e-signature system must include rigorous mechanisms for assuring that the person who completes the e-signing process is actually the intended party to the contract. This needs to be accomplished in a manner that firmly establishes proof-of-identity but also avoids imposing mechanisms that are too cumbersome or complex for most signers (such as requiring signers to create their own PKI digital certificates). In addition, the system should provide the sender with multiple levels of authentication in order to allow tailoring of the proof-of-identity methods to fit their specific business requirements.

"Proof" issues associated with electronic contracting present some challenging questions without a system to manage the contracting process. Imagine the following scenario:

> Tom sends Bob a plain-text e-mail that says "Bob, would you like to buy my boat for $6,000? Your friend, Tom." Bob replies with a plain-text e-mail: "Yes, I'd like to. Regards, Bob."

Under ordinary US law, **Tom and Bob have formed a contract**. There is an offer (Tom's e-mail), acceptance (Bob's e-mail), and consideration (the promised exchange of Boat and money). This is a sale of goods valued over $500, so a signed writing is required; per E-SIGN and UETA Tom's plaintext "Tom" and Bob's plaintext "Bob"—or even their e-mail headers—will meet the signature requirement, and the e-mail will serve as a writing. Let's assume there are no applicable defenses (both of the parties were capable of contracting, etc.). The contract law analysis is easy: there is a valid, enforceable contract.

But, what if Bob claimed that he never sent the message at all? Once Bob denies that he sent the message, Tom will have the burden of proving to a court that in fact it was Bob who contracted with him, and what the substance of their agreement was. In this scenario such a burden would be difficult, but not necessarily impossible, to meet. Tom could, for example, subpoena server logs and determine that the message in fact came from Bob's computer[1] ; he could get testimony from, say, Bob's co-workers that he was sitting at his desk at the time that the message was sent. As a practical matter, under this scenario Tom would probably not be inclined to go to such lengths to enforce the agreement, because Tom is saddled with the burden of proving several things including:

» Bob was the one who signed the agreement
» The contract substance was clear and has not been modified, such as the amount of $6,000 was the agreement,
» Bob signed the contract on a particular date

1 Server logs & agreement links have been used to positively enforce electronic contracts, as with several cases, including Caspi v. The Microsoft Network LLC, Spera vs. AOL, where they are presented correctly, and prior to the event.

If Tom thought the risk of being unable to enforce the contract via email was too high, he could use a more robust electronic process with Bob. For example, he could require that Bob view and sign the document using a digital signature system like DocuSign that provided an audit trail, security, and user authentication.

Note that use of the digital signature system would not change the contract law analysis: digital signature or not, Tom and Bob have a contract. But use of a digital signature system that was designed to provide an audit trail, will make Tom's job of proving the contract easier, and make Bob's denial less credible, and much less likely.

Anyone engaging in electronic contracting will need to make a careful risk/benefit determination around questions of proof. A party to an electronic contract may have to go before a judge and show (a) that there was, in fact, a contract formed – i.e., there was an offer, and acceptance, and consideration, etc.; (b) what the substance of the contract was; and (c) who the contracting parties were.

Some methods of electronic contracting, such as use of CA-authenticated digital signatures, may make proving these points easy. However, the cost and hassle of requiring Bob to buy a digital certificate and the software required to view and sign documents make it unreasonable.

Non-repudiation

Non-repudiation is an important concept when it comes to signing any legal documents. Lawyers use the term 'repudiate' to mean to *reject the validity or authority of something*. When we sign an agreement we seek to have that agreement be "non-repudiable' or done in such a way as to make it impossible for someone to deny they signed for one reason or another. Attempted repudiation of facts around the signing a contract can include:

» Repudiation of Content – "Someone made changes without agreement"
» Repudiation of Signer – "I did not sign that/that is not my signature"
» Repudiation of Change – "Somebody changed the document after I signed."
» Repudiation of Date – "I signed that before or after the indicated date"
» Repudiation of Intent – "I did not see that part of the contract!"

Therefore, a robust e-signature process needs to provide a strong audit trail that captures the content of the document, eliminates the risk of subsequent changes and then creates an indisputable association between the contract, the date signed, and the signing parties.

"Signed writing" Requirements

"Signed writing" requirements have caused a great deal of confusion in connection with electronic contracting – probably unnecessarily.

The fact is, most contracts require neither a "signature" nor a "writing" to be valid. There are a small number of exceptions to this general rule, usually based on a policy of requiring more proof in connection with contracts where there is a higher degree of fraud risk or of high-stakes misunderstanding. Some examples of contracts that require a "signed writing" are contracts for:

- Sales of goods priced over $500
- Transfers of land
- Obligations that cannot be performed in less than one year
- Assignments (but not licenses) of some intellectual property

Courts have tended to construe the signed writing requirement very broadly, allowing; for example, fax headers or pre-printed letterhead to serve as a "signature", and it is likely the courts would have treated e-mail headers or plain-text e-mail signatures in a similar manner, however, E-SIGN and UETA have made this question moot. As described above, under E-SIGN and UETA "signature" and "writing" requirements are very easily met electronically.

The bottom line is that, despite the conventional wisdom to the contrary, when doing electronic contracting under U.S. law, meeting legal "signature" or "writing" requirements is not a significant issue, particularly in light of E-SIGN and UETA.

E-SIGN does provide for some special rules about "written notice" requirements in connection with certain legally required consumer disclosures, applicable, for example, to the insurance and banking industries called the 'consumer consent provision [2]'. Under these rules, consumers must be provided with an option to 'opt out' of an electronic transaction if they wish, and must agree to proceeding with an electronic agreement.

It is *really* a Business Decision!

However, many online businesses rely on "click-through" contracts where users self-report their identity. These businesses can still make good proof arguments: by keeping careful records they can show how they formed contracts with users and show the substance of the contracts; they will have some evidence of user identity. But these businesses presumably have made a decision to forgo the proof benefits accorded by more robust authentication techniques after weighing these benefits, the associated costs, and the risks and consequences associated with potential unenforceability of their electronic contracts.

The bottom line is that it is easy to form a contract electronically, and electronic contracts may be formed a variety of ways. But it may be difficult to prove an electronic contract in the event of a dispute. It is important to take this into account when engaging in electronic contracting, and to scale authentication techniques in accordance with the risk of unenforceability and the consequences if the contract were to be unenforceable.

2 Section 101(c)(1)(C)(ii) states that a consumer's consent to receive electronic records is valid only if the consumer "consents electronically or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent."

ESIGN/UETA Legislation Overview

On June 30, 2000, President Clinton signed into law the Electronic Signature In Global and National Commerce Act (E-SIGN Act). E-SIGN became effective in the United States on October 1, 2000. E-SIGN implements a national uniform standard (the 'floor') for all electronic transactions and encourages the use of electronic signatures, electronic contracts and electronic records by providing legal certainty for these instruments when signatories comply with its standards. They broadly define Electronic Signatures as *"an electronic sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."* This drafting was intentional to allow many types of technology (E-SIGN is technology neutral) and methods for signing electronically, while maintaining legal compliance.

By definition then, an electronic signature can be just about anything produced by *electronic means (e.g., a symbol, result, or consequence),* which has been created electronically in order to demonstrate a party's intent to sign an electronic record. Specific examples of electronic signing include, entering a password or personal information number (PIN), typing a name where indicated (or prompted) via computer keypad, responding to telephone keypad agreements (e.g., "press 3 to agree or 5 to hear this menu again"), *responding to click agreements, even responding to an email thread can constitute a digital signature*. In several cases, courts have upheld server logs as evidence of contract agreement.

This new legislation effectively solves the 'signed writing' problem, by providing provisions that make electronic communication and contracts equivalent to their paper cousins:

- "Electronic Signature" is defined as 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
- "Electronic Record" means a created record generated, sent, communicated, received, or stored by electronic means.
- A contract may not be denied legal effect or enforceability solely because of its electronic form;
- If a law requires a record to be in writing, an electronic record satisfies the law.
- If a law requires a signature, an electronic signature satisfies the law.

In addition, this legislation pre-empted the inconsistent State laws that were technology-centric around PKI-specific 'digital signature' requirements. The challenge in some cases is to prove if the state law is indeed subject to pre-emption. This is a remaining 'grey area' of the new legislation. *However, there is no known case law that does not uphold e-contracts specifically because of a lack of state law. In nearly every case, the courts referred to basic contract law to resolve the matter.*

DocuSign®
The fastest way to get a signature.®

WHITE PAPER

What is NOT allowed to be signed with e-contracting?

ESIGN and UETA define several contracts that are not covered by the legislation. This is not to say they are invalid as electronic transactions, they are simply not part of the ESIGN legislation. This list includes:

» Wills, codicils or testamentary trusts

» UCC transactions (other than Article 2 and Article 2A transactions) generally are excluded, in the UETA (and NCUETA as per N.C.G.S. section 66-313(b)(2)), but in appropriate instances the UCC already provides or will provide for electronic treatment.

» Any notice of cancellation or termination of utility service or to any notice of default, acceleration, repossession, foreclosure or eviction (or the Right to Cure) under a credit agreement secured by or a lease of a "private residence for an individual.

UCC Exclusions & Transferable Records

To understand the meaning of the UCC exclusions, a brief overview of the UCC Code is needed. As UCC transactions other than article 2, and 2A are excluded from coverage by ESIGN or UETA, the sections detailing management of 'Transferable Records' and refers to documents which would be considered a 'note' under UCC article 3, and further states that this note may be executed using an electronic signature.

It is easy to confuse the UCC exclusions. The table below discusses how different UCC sections relate to electronic signature solutions.

UCC Code and Electronic Signature Systems			
UCC Code	**Electronic Records Use**	**Example Transaction**	**DocuSign Express**
Article1.-GeneralProvisions	NA	General	NA
1-107	Allowed	Right Afer Breech	Version 1
1-206	Allowed	Signed Writing Enforcement	Version 1
Article2.Sales	Allowed	Sales Contracts	Version 1
Article2A.Leases	Allowed	Lease Agreements	Version 1
Article3.Negotiable Instruments	With Transferrable Records Capability	Mortgage Notes	Version 1.1
Article4.BankDeposits	NA	Checks	NA
Article4A.FundsTransfers	NA	EFT Systems	NA
Article5.LettersofCredit	With Transferrable Records Capability	Bank Letter of Credit	Version 1.1
Article6.BulkTransfers	NA	Liquidation Notice	NA
Article7.WarehouseReceipts,BillsofLadingandOtherDocumentsofTitle	With Transferrable Records Capability	Vehicle Title	Version 1.1
Article8.InvestmentSecurities	NA	Securities	NA
Article9.SecuredTransactions	NA	???	NA

Given the UCC exclusions, in order to execute a 'note' electronically as DocuSign Version 1.1 does, the following requirements must be met:

The system must be able to create a process which proves that:

1. the record is unalterable;
2. a person can have control over a transferable record;
3. a single authoritative copy can be shown to exist, which is unique and identifiable;
4. the authoritative copy indicates that the record has been transferred, and the person to which the record has been most recently transferred;
5. the authoritative copy is communicated to and maintained by the person asserting control;
6. copies of the authoritative record can only be made with permission of the person asserting control;
7. each copy made, and any copy of a copy is readily identifiable as a copy, and that it is not the authoritative copy;
8. any revision of the authoritative copy is readily identified as authorized or unauthorized.

The law stipulates that if the electronic system enables such management of the note in electronic format, the electronic record shall have the same rights and defenses as equivalent paper records under the UCC, extending electronic coverage.

Considering State legislation

So, with the passage of UETA and ESIGN, how do we consider state-level legislation as it pertains to electronic contracting? Many states have their own legislation, some focused on 'digital signatures' and certificate authorities, some adopting 'technology neutral' UETA. Either way, there are two distinct bodies of legislation in most states. One set of laws deals with 'Digital Certificates' – and the certificate authorities to regulate the ability of CA companies to establish 'open PKI' certificates for individuals that other companies will rely on. The second set of laws are more targeted at the process of electronic contracting, and are the focus of the DocuSign method because DocuSign does not require the use of complex PKI.

How do State Laws relate to UETA and ESIGN?

State laws around the use of electronic contracts vary. The congressional strategy with UETA and ESIGN was to force states into adopting some uniform rules so that interstate commerce could evolve online. They did this by creating some 'pre-empting' rules for the new legislation that provides conditional federal preemption of state law under most cases. A state law, regulation or rule will not be preempted if it:

(1) Constitutes an enactment or adoption of UETA and is not "inconsistent" with ESIGN or;

(2) Specifies alternative procedures or requirements for using or accepting e-signatures or e-records and

- a. Is not inconsistent with ESIGN,
- b. Does not require or accord greater legal status or effect to specific technologies, and,
- c. Makes specific reference to ESIGN if adopted after the enactment of ESIGN.

Nearly all states either adopted UETA, or have provisions for recognizing digitally executed contracts. There is some common language used by several states that have not adopted UETA per se - written as follows:

Georgia/NY: "Authorizes Electronic Signatures with specified authentication attributes only. 'Electronic signature' means:

- An electronic or digital method executed or adopted by a party with the intent to be bound by or to authenticate a record, which is
- Unique to the person using it,
- Is capable of verification, is under the sole control of the person using it, and
- Is linked to data in such a manner that if the data are changed the electronic signature is invalidated."

South Carolina: "An electronic signature is deemed to be secure if:

(1) it is created by application of a security procedure that is commercially reasonable and agreed to by the parties;

(2) the electronic signature can be verified by use of a procedure that is recognized and approved [pursuant to statute]; or

(3) when not previously agreed to by the parties, the electronic signature is:

a. Unique to the party using it;

b. Capable of identifying such party;

c. Created in a manner or using a means under the sole control of the party using it; and

d. Linked to the electronic record to which it relates, in a manner such that, if the record is changed, the electronic signature is invalidated."

Despite the slight differences across the states, as of 2003, there is enough case law to begin to allow businesses to feel more comfortable that in the event of a dispute over an electronic contract, if it is done correctly, the contract will be found valid. Further, DocuSign process adheres to UETA and these example case law processes.

The Problem with Digital Certificates

As many companies have seen, the big 'digital signature' revolution which was supposed to take place in early 2001-2002 never happened. Companies have gone out of business trying to create solutions that allow digital certificates to be the foundation upon online signing because the solution was so expensive and confusing.

Although many states have adopted legislation regulating the CA and PKI process, and even suggesting that these are the only ways an electronic contract can be processed, the fundamental issue is that PKI – or more specifically Pubic Key Infrastructure is flawed to a point that it just does not work for a large percentage of the businesses – especially businesses who need to send documents to their clients and customers.

The fact is that PKI addresses encryption, and not the process of signing and is better suited to a task of securing servers than documents or signatures. Further, the 'open' PKI process sets itself up for failure, while other ESIGN compliant server-based methods specifically designed for use for specific business purposes are much less likely to be compromised.

What is truly amazing is the sheer volume of 'e-contracting' that happens every day – **without digital certificates, without complex software**. Every web site agreement, ever online broker, and most ISPs have you e-sign contracts. They are so simple you may not even know you have signed, but every time you click on an "agree" button on a web site, that act is deemed to have the same effect and be as enforceable as you signing your name at the bottom of a contract.

The fact is that PKI as a way to create global online ID's for signers has proven too heavy for most business e-contracting.

Problems with PKI Compared to DocuSign

The open PKI scenario implicates considerable liability risk. Proponents of the open model, enamored with what digital signatures can potentially accomplish, have attributed this risk to flaws in the existing legal regime that must be addressed legislatively. This conclusion is wrong. The liability exposure faced by CAs under the open PKI model is the product of a business model that cannot internalize the costs of the inevitable fraud that will result under any public key-based system. The resulting liability problem is unlikely to be solved at all in the open PKI model, and certainly cannot be solved with any one-size-fits-all legislative solution.

Here is one aspect of the problem: if criminals can obtain something valuable by expropriating an individual's private key, they will. There is simply no practical way to keep private encryption keys truly secure. Proponents of digital signature technology frequently mention the concept of storing private keys on tamper-proof smart cards. While smart cards, particularly smart cards that incorporated biometric measures designed to prevent unauthorized use of a misappropriated card, would undoubtedly promote the security of private keys, at this point this is simply wishful thinking - this type of smart card is not commercially deployed in any meaningful way, and is unlikely to be in the foreseeable future. There is currently no realistic way to truly secure private keys, and this problem is going to get worse before it gets better.

Private keys will be expropriated, and third parties will rely on ostensibly valid but fraudulent documents and suffer losses. The aggregate losses could be quite sizable, judging from analogous contexts: MasterCard and Visa lose over $ 1 billion per year to fraud; phone companies claim to lose $ 3 billion a year to fraud; in the city of Los Angeles alone fraudulent real estate document filing is said to have cost $ 131 million in a twenty-seven month period.[3] Who will bear these losses?

There are three primary choices:

1) The relying party;
2) The individual whose key was used to sign the document; or
3) The CA who performed the initial binding.

Under the Utah Act, the individual whose key was used to sign the document bears unlimited liability if they failed to exercise "reasonable care" to protect their private key, (which is not well defined.) The Act also imposes difficult evidentiary burdens on the individual. So, if a subscriber - named "John Signer," just to put

3 In 1994 MasterCard reported a loss of $ 486 million due to credit card fraud; Visa's fraud loss was $ 645 million. Robert Jennings, Fraud is Stealing Holiday Joy from Credit Card Companies, American Banker, Dec. 7, 1995, at 1. Phone companies estimate that they lose about $ 3 billion to calling card fraud and other types of fraud. Peter Sinton, Visa Has Sights Set on Credit Card Fraud, San Francisco Chronicle, Sept. 14, 1994, at B-1. L.A. County District Attorney Gil Garcetti estimated that county residents were cheated out of $ 131 million between July 1990 and November 1992. Timothy J. Moroney, Review of Selected 1995 California Legislation, 27 Pac. L.J. 451, 452 (1996).

things in perspective - does not exercise reasonable care, and her key is stolen resulting in losses totaling $ 25,000 prior to revocation of her key, that subscriber bears the loss - i.e., John Signer loses his house. Or, if John Signer does exercise reasonable care and her key is still misappropriated, he must present a court with "clear and convincing" evidence (the standard under the Utah Act) to overcome the presumption that she in fact signed a document signed with her digital signature. In either case, the result does not comport with well-established consumer protection laws (compare with the legislatively-imposed $ 50 consumer liability limit for credit card losses, or the fact that one cannot be bound by a fraudulent handwritten signature). Moreover, no rational consumer would agree to accept this level of risk in a marketplace transaction. The benefits of having a certificate simply do not outweigh the very real possibility of facing extraordinarily large un-reimbursed losses.

From a practical perspective, the following are systemic issues that distributed PKI based signing systems have, which make it a much less capable system for signing. The following table compares a distributed PKI system (where documents are encrypted and sent via email) to DocuSign's patented server-based online signing service:

Requirement	PKI System Problems	DocuSign Alternative
1. Virus Exposure	Documents sent as email attachments. Issues with firewalls and viruses.	File stored on a secured server rather than sending it to recipients. No issues with viruses.
2. Event Notification	Unable to notify Senders when documents are viewed, signed, or declined. Tracking control is lost because documents are distributed as attachments. Senders only know when the signing is done when the document is sent back in email.	Instant event notification for all parties to a transaction, such as delivery, failure to deliver (with ability to correct), receipt, approval, and signature or decline, along with reason for decline.
3. Audit Trail	Incomplete audit trail. There is no way to assure 100% audit coverage of the file once it is sent.	100% audit trail - around the document, and around each person who accesses the document. Audit trail is hashed and secured by the system.
4. Multiple Signers	In the case of multiple signers, the sender must send multiple files – each person will be signing one copy in counterparts	All signers sign the same document. Each signer can see the others signatures so are comfortable they are signing the same file. There is no need to 'combine' multiple documents signed in counterparts.
5. Technical Barriers	Require a digital certificate be installed on the recipient's PC. Financial cost, takes time to secure and process is often confusing.	Recipients only need email and a web browser to sign.
6. Signing Location	Require a particular PC be used by the recipient. Cannot sign from 'just any PC'.	The recipient can sign from any PC, (or browser-enabled device).

Requirement	PKI System Problems	DocuSign Alternative
7. Person or PC?	PKI is really just password protection to access and use a digital certificate. You don't know that a specific person signed only that a specific PC unlocked the file.	The specific person (recipient) is authenticated, not the PC. Password protection is also used but additional authentications can be added at any time, for any document.
8. More Software	Requires specific software that works with specific applications to allow addition of the digital signature to a document.	No requirement for any specific software – can send and sign any Windows document that can be printed.
9. Document Integrity	When a document is unlocked to sign, and a digital signature attached, the underlying document HASH is modified.	The underlying file with the original HASH is stored. The signing process does not modify this therefore better preserving document originality.
10. Point of Failure	Digital Certificate creates a 'single point of failure'. If a person obtains it fraudulently, everyone can be defrauded by that person.	No single point of failure. Each person authenticates separately. Different levels of authentication are available with each new relationship (as in the real world). Just because a person is authenticated with one company, does not mean other companies need to trust those authentications – they can set up their own.
11. ESIGN Compliance	Does not manage the ESIGN disclosure infrastructure required to comply with consumer online signing. Makes it hard to sign documents with end-users without other specialized processes and tools in place. Often, these systems operate without the protection of the Federal ESIGN Act.	Integrates the creation, distribution, and management of ESIGN disclosures with each signer as part of the Online Signing Service.
12. Liability Level	Little user protection in the eyes of the law. A lost of stolen certificate leaves the owner 100% liable for the fraud.	If a user's account is compromised, the owner is only liable for up to the limit of credit card fraud – which is about $50 in most states.
13. Sign Where?	Without specialized software, does not ensure the right person signs on the right location in a document. No safeguards to prevent signer from missing signatures spots. They often just sign the 'whole file'.	Each person assured to sign on the right location in the document. Both the signature and location of the signature in the document are recorded for maximum legal intent. Signers directed to all signature locations and prompted if omissions before returning the document..
14. After Signing	No ability to manage documents after they have been signed.	Option to securely archive signed documents for years – keeping them under 100% audit.

How DocuSign Contracts meet the law

DocuSign meets the legal requirements for e-contacting by providing a structured process for reviewing, and signing any document in compliance with contract law, ESIGN/UETA, and most importantly, creating a strong means of 'proof'. DocuSign does this with extremely simple tools – making the creation of legally binding contracts electronically actually EASIER than printing, and actually more reliable.

The DocuSign process provides:

1. **Content Control –** DocuSign encrypts and locks each file submitted for signatures into the DocuSign Vault. This document can be proven not to have been modified and is time stamped and audited 100% of the time.

2. **Secure Signatures –** DocuSign creates a unique signature for each system user, and ensures that only that user can apply their signature. This signature is locked once created, and the user cannot change it.

3. **Authentication of Signers –** Each contract originator can determine the best method of authentication of their customer. Since they are not relying on someone else to validate the customer, the contain their risk of fraud
   a. **Email authentication –** essentially working with a known person, that has a reliable history, or someone who was proven ID in person, or through some other process as determined by the business
   b. **Secret work authentication –** eliminates the possibility of hackers impersonating the signers
   c. **Out of Wallet Questions –** a very strong filter to determine the true identity of the signers. This will only be used in cases where the document sender does not know the signer.

   Each of these authentication methods creates a 'trail' showing that a particular person was in fact the individual in the transaction, and is superior to simple 'server logs' which have already proven to be enough to enforce contracts in several prior rulings. (See case law section).

4. **Notice of e-contracting –** As per ESIGN and many state laws, the signer is required to review and consent to a disclosure statement in which they 'agree' to the process of singing, and also agree to waive the need to sign on paper. This is an important aspect of enforceability.

5. **Audit Trail Elements –** The DocuSign Audit Manger identifies each person to the transaction, and keeps a record of every document action, view, sign, and print made. This audit trail information is also hashed so changes cannot be made to past recorded events.

6. **Intent –** The DocuSign system enables signers to place initials and signature stamps in any document location, enforcing the ability to show that the signer read and initialed different sections of the document. Further, the system requires the signer re-enter their unique password and a PIN to digitally sign the contract. This is all part of the audit trail.

7. **User Determination of 'Authoritative Copy' options –** Once signed, each signer can print a local copy for their records. As ESIGN stipulates, using a digital contracting process has requirements for access to the contract. DocuSign makes this easy by providing several options:

   a. Signers agree to eliminate the digital copy, and nominate the printed-paper copies each has as the authoritative copy. This removes the online version of the contract, but retains a 'receipt' of the transaction that is a list of the transaction details.
   b. Signers agree to archive the digital copy in the DocuSign server, creating a central 'master' which can serve as a single point of reference for future contract discussions.
   c. Signers can also save a locked PDF file of the contract, along with signing data on their computer for future referral. This locked PDF can also serve as a strong evidence of contract signing.

Summary

In summary, DocuSign has been designed to conform with all of the tenets of common contract law and rules of evidence, thereby providing an easy to use and legally enforceable process that is mirrored in the paper world. In addition, it has been designed to comply with UETA and E-SIGN, and in fact exceeds these requirements.

An in-depth legal review and analysis of DocuSign, conducted by the leading business law firm, Lord, Bissell & Brook has determined the following:

"The DS System is an effective tool for creating electronic signatures and records under applicable electronic signature law, and might in some cases mitigate certain risks associated with a contracting process to levels at or below that of a process using traditional wet ink and paper."

Today, consumers sign online contracts every day - agreements on web sites, online stock trading accounts, etc. DocuSign extends this model to any document that needs to be sent for signature and delivers the secure knowledge that the agreement will have the same legal effect as if paper had been sent.

By addressing and solving the key factors needed for enforceable e-signatures, those of intent, proof of identity, and non-repudiation, DocuSign provides an economical and easily deployable solution that does not require expensive software or digital certificates. DocuSign efficiently puts control over the authentication process into the hands of our corporate customers; giving them the tools to easily deploy legally enforceable e-signature processes that meet their real-world business needs.

DocuSign legal Framework

To summarize, DocuSign has been framed after common contract law, and rules of evidence, and provides a process that is mirrored in the paper world. In addition, it has been designed to comply with UETA and ESIGN, and in fact exceeds the requirements.

DocuSign is a 'closed PKI' model, where the business establishes their own levels of authentication with their clients for the purpose of signing, and provides a clear audit trail of events surrounding the signing in a way that ensures non-repudiation.

DocuSign legal benefits are:

» Supported by e-contracting case law.

» Less risky than Open PKI because each business decides on the authentication for their customers, and it provides a complete solution for any document.

» Focused on solving the business problems of proof, rather than 'technology' of encryption. DocuSign provides the audit trail needed to prove who, when, what was signed.

» Flexible options enable users to deploy easily, and does not require expensive software or certificates

» Creates contracts which can be stored online, or printed as legally binding agreements from any desktop document (MS Word, Fax, etc)

» Much faster contract signings are possible because there is no need to physically print copies and send them for signature.

» Much lower cost than is associated with printing, "FedExing", etc.

This white paper has shown that documents signed using the DocuSign process are legally binding, enforceable, and easier to manage than traditional paper processes, and the DocuSign system is a more complete solution than distributed PKI technology.

This document contains information found in white papers from Brian Casey & Patrick Hatfield at Lord, Bissell & Brooks, and Brad Biddle "A short history of "digital signature" and "electronic signature" legislation, as well as state legislation.

Appendix One

American Bar Association Recommendation for e-contracts

The following is taken from the American Bar Association's white paper titled: "Click-through Agreements: Strategies for Avoiding Disputes on Validity of Assent". The Working Group on Electronic Contracting Practices, Electronic-Commerce Subcommittee of the Cyberspace Law Committee, Business Law Section, published this document in 2002.

According to the ABA, case law now provides a pattern for strong use of online e-contracting procedures to ensure enforceability. DocuSign embodies these suggestions in our e-contracting process:

Opportunity to Review Terms

1. **Viewing of Terms Before Assent:** The User should not have the option of manifesting assent without having been presented with the terms of the proposed agreement, which should either appear automatically or appear when the User clicks on an icon or hyperlink that is clearly labeled and easily found. *DocuSign requires agreement prior to account creation.*

2. **Assent Before Access to Governed Item:** The User should not be able to gain access to or rights in the website, software, information, property, or services governed by the proposed agreement without first assenting to the terms of the agreement. *DocuSign requires agreement prior to account creation.*

3. **Ease of Viewing Terms:** The program operating the click-through agreement should give the User sufficient opportunity to review the proposed agreement terms before proceeding. The User should be able to read the terms at his or her own pace-, if the terms occupy more than one computer screen, the User should be able to navigate forwards and backwards within the terms by scrolling or changing pages. *DocuSign enables the signer to scroll up and down, and will not allow agreement until the document has been scrolled to the bottom.*

4. **Continued Ability to View Terms:** Once the User views the terms, the User should be able to review the terms at later stages of the assent process. *DocuSign enables the signer to print the assent and return it to the sending company if so required.*

Display of Terms

5. **Format and Content:** The format and content of the terms must comply with applicable laws as to notice, disclosure language, conspicuousness, and other format requirements. The terms should be clear and readable, in legible font. If the law requires specific assent to a particular type of term, the format of the assent process should comply with that requirement. DocuSign consent notice is viewable in any browser.
6. **Consistency with Information Elsewhere:** Information provided to the User elsewhere should not contradict the agreement terms or render the agreement ambiguous.

Acceptance or Rejection of Terms

7. **Choice Between Assent and Rejection:** The User should be given a clear Am between assenting to the terms or rejecting them. That choice should occur at the end of the process when the User's assent is requested. *DocuSign provides the ability to 'opt out' of the online signing.*

8. **Clear Words of Assent or Rejection:** The User's words of assent or rejection should be clear and unambiguous. (a) Examples of clear words of assent include "Yes" (in response to a question about User's assent), "I agree," " I accept," "I consent," or "I assent." *DocuSign uses 'I agree'.*

9. **Clear Method of Assent or Rejection:** The User's method of signifying assent ion should be clear and unambiguous. Examples include clicking a button or icon containing the words of assent or rejection, or typing in the specified words of assent or rejection. *DocuSign uses 'I agree' button on the bottom of the page.*

10. **Consequences of Assent or Rejection:** If the User rejects the proposed agreement terms, that action should have the consequence of preventing the User from getting whatever the click-through agreement is granting the User. The User should not be able to complete the transaction without agreeing to the terms. For example, if the click-through agreement would grant the User use of a website, software, or particular data, the consequence of the User's rejection of the proposed terms should be to bar the User from that use. Likewise, if the click-through agreement would give the User rights to goods or services, the consequence of the User's rejection of the proposed terms should be to eject the User out of the ordering process. On the other hand, if the User assents to the proposed agreement terms, the User should be granted access to whatever is promised in the agreement without having to assent to additional terms (aside from those that the User specifies in the ordering process). *DocuSign cancels the signers login process, and returns a message to the sender if the signer has rejected online signing.*

11. **Notice of Consequences of Assent or Rejection:** Immediately preceding the place where the User signifies assent or rejection, a statement should draw the User's attention to the consequences of assent and rejection. Examples of notice of assent consequences include: "By clicking 'Yes' below you acknowledge that you have read, understand, and agree to be bound by the terms above" or "These terms are a legal contract that will bind both of us as soon as you click the following assent button." Examples of notice of rejection consequences include: "if you reject the proposed terms above, you will be denied access to the [Web site, software, product, services] that we are offering to you." *DocuSign informs the signer that rejecting will result in a cessation of the signer's login process, and will return a message to the sender if the signer has rejected online signing.*

Opportunity to Correct Errors

12. **Correction Process**: The assent process should provide a reasonable method to avoid, or to detect and correct, errors likely to be made by the User in the assent process. A summary of an online order preceding assent is one such means. *DocuSign allows and recommends the signer print and save a copy of the assent.*

Keeping Records to Prove Assent

13. **Accurate Records:** Maintain accurate records of the content and format of the electronic agreement process, documenting what steps the User had to take in order to gain access to particular items and what version of the agreement was in effect at the time. If necessary, for proof of performance, link the User's identity to his or her assent by maintaining accurate records of the User's identifying information, the User's electronic assent to the terms, and the version of the terms to which the User assented. Be sure to comply with applicable privacy laws. *DocuSign Audit manger captures all user activity, and ensures only authorized files are visible.*

14. **Retention and Enforceability:** To meet any legal requirement that a record of the agreement be provided, sent, or delivered, the sender must ensure that any electronic record is capable of retention by the recipient. In addition, for an electronic record to be enforceable against the recipient, the sender cannot inhibit the recipient's ability to print or store the electronic record. *DocuSign enables any signer to print a copy locally and/or retain access to an online archived copy.*

15. **Accuracy and Accessibility after the Assent Process:** If applicable law requires retention of a record of information relating to the transaction, ensure that the electronic record accurately reflects the information and, if required, remains accessible to all persons entitled to access by rule of law for the period required by the rule of law in a form capable of accurate reproduction for later reference. *DocuSign Audit manager, and encryption scheme ensure that any stored documents cannot be modified. Further, the signers all print a copy along with a digest record of the transaction for filing on their own system.*

Appendix Two

Validity of Assent in Click-through Agreements

Cases and Other Disputes

America Online, Inc. v Booker, No. 3D00-2020, 2001 WL 98614 (Fla. Dist. Ct. App. Feb. 7, 2001) (electronic agreement with Internet service provider *implicitly held valid* as the court enforced the forum selection clause in a "freely negotiated agreement" that has not been shown to be "unreasonable or unjust;" no indication whether agreement was express via a click-through or simply implied in some way).

America Online, Inc. v. Super. Ct. (In re Mendoza), 108 Cal. Rptr. 2d 699 (Ct. App. 2001), (using the standard of review involving the most deferential abuse of discretion and shifting the burden of proof to party seeking to uphold forum selection clause contrary to California Consumers Legal Remedies Act (CCLRA), the court of appeals affirmed the trial court by invalidating Virginia forum selection clause in click-through agreement, based on public policy in (i) anti-waiver provision in CCLRA, and (ii) California consumer protection provisions, which would be substantially diminished in Virginia, *but court of appeals did not explicitly rule on the validity of the click-through agreement),aff'g*

Mendoza v. America Online, Inc., No. 827047-2 (Cal. Super. Ct. Sept. 25, 2000) (unreported), *available at* http://caselaw.lp.findlaw.com/data2/californiastatecases/ a092813.pdf (forum selection clause in click-through agreement during installation process on CD-ROM held unfair and unreasonable because clause was not negotiated at arm's length, was in standard form contract, was not readily identifiable by plaintiff due to small text and location of clause at conclusion of agreement, and was contrary to California public policy giving its citizens specific and meaningful remedies that are readily accessible and available; defendant did not meet burden of showing that the latter element was not diminished under Virginia law).

Caspi v. Microsoft Network, L.L.C., 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999) (clickthrough agreement *expressly held valid* where network subscribers could click either box saying "I Agree" or "I Don't Agree" at any time while scrolling the adjacent terms of the membership agreement, which included forum selection clause at issue; registration occurred and charges were incurred after subscriber clicked "I Agree"; court drew analogy to plaintiffs precontractual opportunity to read the fine-print terms in Carnival Cruise Lines and refused to treat electronic and paper presentations of terms differently).

Celmins v. America Online, Inc., 748 So. 2d 1041 (Fla. Ct. App. 1999) (electronic agreement with Internet service provider implicitly held valid as the court enforced the forum selection clause; no indication whether it was click-through or click-free).

CompUSA Agrees to Discontinue Practice of Placing Disclosures Behind Several Links, 6 ELECTRONIC COM. & L. RPT. (BNA) 562 (May 30, 2001) (settlement with New York attorney general) (deceptive business claim for failure to clearly and conspicuously disclose that $400 rebate was conditioned on buyer subscribing to three years of Internet service and that early termination of that subscription carried a penalty of $250 to $450; 5 6 those conditions were viewable only after buyer followed three and four layers of hyperlinks past the homepage).

Compuserve, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996) (online Shareware Registration Agreement in which User typed "agree" was *implicitly held valid* and used as one of several contacts used to justify holding subscriber subject to personal jurisdiction in service provider's home state; no details on format or assent method).

Groff v. America Online, Inc., No. PC 97-0331, 1998 WL 307001 (R.I. Super. Ct. May 27, 1998) (click-through agreement with internet service provider *implicitly held valid* where subscriber could not have enrolled without clicking the "I agree" button next to the "read me" button or the "I agree" button next to the "I disagree" button at the conclusion of the agreement, which contained the forum selection clause at issue).

Hotmail Corp. v. Van$ Money Pie, Inc., Nos. C-98JW PVT ENE, C 98-20064JW, 1998 WL 388389 (N.D. Cal. Apr. 16, 1998) (click-through agreement *implicitly held valid* in preliminary injunction granted based on likely violation of click-through subscription agreement with internet service provider, as well as other causes of action; no details on format or assent method).

Lieschke v. RealNetworks, Inc., Nos. 99 C 7274, 99 C 7380, 2000 WL 198424 (N.D. Ill. Feb. 11, 2000) (click-through agreement *implicitly held valid* in court's stay of court proceedings in favor of arbitration, where arbitration clause was contained in click through agreement on Website where Users could download software to play and record music, after agreeing to license agreement; no details on format or assent method).

Pollstar v. Gigmania Ltd., No. CIV-F-00-5671 RECSMS, 2000 WL 33266437 (E.D. Cal. Oct. 17, 2000) (court denied motion to dismiss by defendant User, who had copied plaintiff's Web site information allegedly protected by browse-wrap license agreement, but also *voiced concern about validity* of license agreement, notice of which appeared in hyperlink "in small gray text on a gray background" to another screen containing text of proposed agreement that did not require User's explicit assent).

In re RealNetworks, Inc., No. 00 C 1366, 2000 WL 631341 (N.D. Ill. May 8, 2000) (clickthrough agreement *expressly held valid* against procedural unconscionability challenge where the contested arbitration clause appeared in final paragraph entitled "Miscellaneous" along with provisions on choice of law and forum selection, in same font as rest of agreement, freely scrollable and viewable without any time restriction; User must agree to online license agreement before it can install software from RealNetworks' Website, but the opinion did not detail the method of assent; court also held that this particular electronic document was a "writing" under the Federal Arbitration Act).

Rudder v. Microsoft Corp., No. 97-CT-046534CP, [1999] 2 C.P.R. (4th) 474, 1999 CarswellOnt 3195 (WL) (Ont. Super. Ct. Justice Oct. 8, 1999) (forum selection clause in click-through contract *expressly held valid* where sign-up procedure required User to accept agreement terms each time they appeared on computer screen, entire agreement could be viewed by scrolling down screen, and terms of agreement were not analogous to fine print; court concerned that it not undermine integrity of electronic agreements; defendant also proved substantial connection to forum and justified clause substantively).

Specht v. Netscape Communications Corp., 150 F. Supp. 2d 585 (S.D.N.Y. 2001) (arbitration clause in licensing agreement *explicitly held invalid* because plaintiff did not assent to what the court called a "browse-wrap agreement" in which User was not required to click on an icon expressing assent to the license, or even view its terms, before downloading the software governed by the alleged agreement; the post-download instruction to "please review and agree to the terms of the Netscape SmartDownload software license agreement before downloading and using the software" was held to be a mere invitation, not a condition to downloading and using the software).

Scott v. Bell Atlantic Corp., 726 N.Y.S.2d 60 (App. Div. 2001) (court granted DSL providers' motion to dismiss pre-certification class action for misrepresentation, holding that *providers were not liable for false or deceptive conduct, breach of warranty,* or breach of contract where the enthusiastic advertising copy elsewhere on the Web site was at odds with disclaimers of service quality in the agreement on the installation CD-ROM).

Williams v. America Online, Inc., No. CIV A. 00-962, 2001 WL 135825 (Mass. Super. Ct. Feb. 8, 2001) (forum selection clause *expressly not upheld* in motion to dismiss a class action lawsuit concerning the installation of a software program in which damage to the User's system occurred before the User reviewed and assented to the agreement, and where the agreement terms were accessible only by twice overriding the default choice of "I Agree" and clicking "Read Now" twice; second ground for ruling was the public policy against requiring Mass. residents with small claims to litigate in Virginia).

Appendix Three

Comparison of E-Sign and Pure UETA

1. **Quality of Drafting.** UETA is better written, and therefore easier to follow and interpret. Compared to E-SIGN, it will give relatively greater certainty to citizens and businesses.
2. **Excluded State Laws.** E-SIGN explicitly excludes from its reach more state laws, but UETA gives the states the flexibility to exclude additional state laws. Compare E-SIGN 103 with UETA 3(a)-(c).

3. **Government Affairs.** UETA covers government affairs, rather than just the commercial transactions] covered by E-SIGN. Compare E-SIGN 101(a), 106(13) and UETA 2(16). Its inclusion of government affairs would appear to provide the Commonwealth's agencies with the enabling legislation that they may need should they choose to conduct their own business electronically. Because many state statutes and regulations implicitly or explicitly require that the government conduct its business in writing, and the enabling legislation for state agencies is silent with respect to electronic activity, UETA provides an essential foundation for the transition to e-government.

4. **Consumer Protections.** UETA does not contain the explicit consumer protection provisions set forth in section 103of> E-SIGN, but it leaves in place existing consumer protection laws and makes clear that they will still apply in electronic transactions. UETA 5(b),(e); 8(a),(b), (d)(1)-(2); 15. E-SIGN anticipates some of the consumer problems unique to electronic transactions, and deals with them explicitly, while UETA does not. (Both Senator Nuciforo's and Senator Magnani's bills incorporate the consumer protection provisions of E-SIGN, thereby remedying this defect in the "pure" UETA. See Nuciforo 3(b)(4) and Magnani 5(e), 17(a)-(c)).

5. **Record retention.** UETA enables parties required to keep written records to have an agent keep the records for them. UETA 12(c) E-SIGN lacks such a provision.

6. **Electronic agents.** UETA is clearer and more specific with respect to this topic. Compare E-SIGN 101(h) and UETA 14.

7. **Insurance.** E-SIGN provides a liability exemption for agents or brokers, see E-SIGN 101(j); UETA does not.

8. **Record retention.** E-SIGN forbids states to impose written record keeping requirements on persons required to keep records of particular transactions, unless the requirement of a written record serves a compelling government interest related to national security or public safety. E-SIGN 101(b)(1); 101(d)(1); 101(d)(3);101(d)()102(c); 104(c)(1); 104(b)(3)(B). UETA would permit states to require paper record keeping but only if they pass a law after UETA is enacted specifically permitting the same. UETA 7(c)(d); 12(f); 12(a)(1)-(2); 12(d)-(e). Given the preemptive effect of E-SIGN, any such after-adopted legislation would probably have to meet E-SIGN's test for written record requirements.

9. **Additional Provisions.** E-SIGN does not contain provisions addressing the following issues, which are addressed in UETA:

a. Temporal application (i.e. what transactions the statute will apply to). UETA 4
b. Parties' ability to vary some of the terms of UETA by agreement. UETA 5, 8(d), 10(4), 15(g)
c. Attribution of electronic signatures. UETA 9(a)-(b)
d. Change or error in electronically conducted transactions. UETA 10
e. Rules governing time and place of sending and receipt of electronic records. UETA 15.
f. Admissibility of electronic records and signatures as evidence. UETA 13.

10. **Transferable records E-SIGN limits transferable records to notes secured by real estate,** while UETA would apply to a broader range of commercial paper. Compare E-SIGN Title II and UETA 16.

11. **Federally-Mandated v. Voluntary State E-Procurement.** E-SIGN appears to require that, where they engage in transactions affecting interstate or foreign commerce with private parties who choose to conduct business electronically, states must use or accept electronic records and signatures in the procurement process (except with respect to a contract to which the state is a party). See E-SIGN 101(b)(2). In other words, E-SIGN appears to require that state governments accept electronic record and signatures on all documents related to procurement processes except for contracts to which the state is a party. E-SIGN 101(b)(2); 102(b); 104(b)(4). (This follows because E-SIGN states, implicitly, in section 101(b)(2), that states are required to accept electronic records or signatures except with respect to contracts to which states are parties. Furthermore, E-SIGN explicitly exempts state procurement from only one of the two requirements that it imposes on states that have not adopted UETA and want to specify alternative means of conducting electronic transactions, see E-SIGN 102(b), and only one of the three requirements imposed on states exercising their interpretive authority by interpreting their laws and regulations in light of E-SIGN, see E-SIGN 104(b)(4). Both of these explicit exemptions for state procurement extend only to E-SIGN's requirement that states adhere to technological neutrality. Thus, provisions of state procurement laws mandating the use of written documents "relating to" procurement transactions are preempted to the same extent as other laws and regulations requiring written documents, except to the extent that they apply to contracts entered by a state and/or specify the technology to be used in the conduct of the procurement process.)By comparison, UETA gives states the option to use and accept electronic records in such circumstances UETA 5(a)-(c), 18.UETA therefore provides states with far more flexibility in determining the degree to which they want to conduct business transactions electronically, and the timeframe during which they will migrate to electronic commerce.

12. **Enabling E-Government.** In addition, optional provisions of UETA, which do not appear in E-SIGN, pertain specifically to states' creation and retention of their own electronic records, conversion of their written records to electronic records, acceptance and distribution of electronic records, and the interoperability of systems adopted by state governments to facilitate E-government. UETA 17-19. While section 17 does not appear to be appropriate because it could result in multiple interpretations of the Records Retention Law by different agencies, sections 18 and 19 may provide needed guidance to state agencies faced with questions about their authority to conduct their own business electronically after UETA.

Appendix Four

Practical Tips and Preliminary Thoughts for Lawyers

These statutes are new, and case law is still forming. We are now in the first stages of a new legal/business process. While the marketplace, transaction parties and government bodies catch up with what these statutes permit and encourage, we offer some practical tips and things to do to ensure legal online contracting.

» Become familiar with the UETA and ESIGN, as well as case law supporting online contracts (attached)
» Stay abreast of the local Register of Deeds and the Secretary of State's efforts to "go electronic."
» Be aware, at the beginning of any transaction, of whether you (or your client) want to rely on the UETA to create contracts electronically—remember, the agreement to proceed electronically "is determined from the context and surrounding circumstances, including the parties conduct." But a valid "electronic signature" must be adopted with "intent to sign":
» A person's clicking on "I AGREE" on an Internet website pretty clearly will form a contract under ESIGN and the UETA. However, much stronger tools should be leveraged where practical. Digital Signing solutions such as DocuSign that enable an auditable process for signing which will easily stand up in court, and which is usable by your customers.
» Think about the possible need to negate an inference that the parties have agreed to create a binding contract by intent inferred from an "electronic course of conduct":
» Be careful to include language on e mailed documents indicating, "Draft" or the some other wording to ensure the emails are not construed as contracts inadvertently.
» Include in e mailed "cover correspondence" that "The attached draft is not in final form and is subject to review and approval of both parties.
» Include in your e mail correspondence that you have no ability to bind your client to any particular transaction.
» Be on the "lookout" for risk-shifting provisions in contracts that contemplate electronic execution and performance, such as "EDI" agreements that may try to 'slip under the door'.

83 Columbia Street, Fourth Floor
Seattle, WA 98104

tel 1.866.219.4318
sales@docusign.com

www.docusign.com