Electronic Contracts and Digital Signatures

By Thomas J. Smedinghoff

Editor's note: An expanded version of the following article was presented at the 1997 ELA Lawyer's Conference. It was based on the author's book, Online Law (New York: Addison-Wesley, 1996).[1] This journal would welcome article submissions by lessors outlining their experiences to date with online transactions.

The ability to create and enforce contracts is essential to a commercial society. Thus, as its business activities move to the electronic or online medium, the contracting process must follow.

For lessors as well as other professionals in the finance industry, new forms of technology accelerate the pace of business. By contracting online, lessors have the potential to improve efficiencies, reduce paperwork, and streamline their operations. Lease offers and acceptances, delivery and acceptance procedures, consents and approvals, and the addition of new equipment schedules are just some of the leasing transactions that may be accomplished online.

At the same time, however, new technologies create challenges for the legal system, which must try to apply existing law in a new context. This article discusses how contracts can be formed online; the fundamentals of online offers and acceptances; legal requirements for electronic contracts; real-time communications and open networks; digital signatures and their legal effects; certification authorities; and the obligations of the parties.

HOW CAN CONTRACTS BE FORMED ONLINE?

Contracts can be formed by oral or written agreement. They can be implied by the conduct of the parties. And, with the advent of online communications, they can be formed electronically. A variety of procedures are available for forming electronic contracts:

- **E-mail.** By exchanging e-mail communications, the parties can create a valid contract. Offers and acceptances may be exchanged entirely by e-mail, or can be combined with paper documents, faxes, and oral discussions.
- **Web Site Forms.** In many cases a Web site operator will offer goods or services for sale, which the customer orders by completing and transmitting an order form displayed on screen. Once the order is accepted by the vendor, a contract is formed. The goods and services may then be physically delivered off-line.
- **Online Mass Market Agreements.** Electronic contracts can also be formed by online conduct. For example, a publisher may offer software or other digital content online, subject to a form agreement. The user's conduct of downloading the content may constitute acceptance of the form agreement.
- **Electronic Data Interchange (EDI).** EDI involves the direct electronic exchange of information between computers; the data is formatted using standard protocols so that it can be implemented directly by the receiving computer. EDI is often used to transmit standard purchase orders, acceptances, invoices, and other records, thus reducing paperwork and the potential for human error. These exchanges (which are sometimes made pursuant to separate EDI trading partner agreements) can create enforceable contracts.
- **Other Forms of Electronic Contracts.** Online technology is changing rapidly and can be expected to accommodate many other online contracting techniques. For example, contracts may be formed through interactive telephone systems, such as orders entered through an automated Touch Tone system.[2] Interactive television, when perfected, may also become a source of electronic contracting. Online business agencies may enable buyers and sellers to negotiate contracts online in a global forum, subject to the forum's private set of rules.[3] Software agents may also be used to enter into binding contracts.

The legal issues relating to these and other forms of online contracts are discussed in the following sections.

ONLINE OFFERS AND ACCEPTANCES

An electronic contract may be made in any manner sufficient to show agreement, including offer and acceptance, or conduct that recognizes the existence of a contract.[4] Typically, a contract is formed when one party makes an offer that is accepted by the other party.

An electronic contract may be made in any manner sufficient to show agreement, including offer and acceptance, or through conduct that recognizes the existence of a contract.

Offers

Contract offers may be made orally, in writing, or by conduct. There is no reason why an electronically transmitted offer should be any less effective than an oral or written one.[5] To be valid, an offer must communicate to the person receiving it that, once the offer is accepted, a contract is created.

Acceptances: E-Mail, Mouseclicks, and Other Methods

An offer may be accepted "in any manner and by any medium reasonable in the circumstances."[6] Typical offline acceptances include written and oral communications as well as acceptance by conduct. Their online counterparts include acceptance by e-mail or other form of electronic message, and by conduct such as clicking on a button or downloading content.

Will the courts consider acceptance by e-mail to be a reasonable practice? If an offer is made by e-mail, one should be able to accept it by the same means.[7] But what if the offer was made by some other method, such as letter or fax? An acceptance does not necessarily have to be sent the same way as the offer.[8] However, because of the special attributes of e-mail, the courts will likely decide each case based on the circumstances.[9] To be certain, it is best to confirm the other person's customary practice before assuming that e-mail responses are appropriate.

Timing of acceptances can be important in determining if there is a binding contract. That is because a offer can generally be revoked if it has not yet been accepted.

What about conduct such as using a mouse to click on a button, entering a symbol or code, or downloading content? Will these be considered proper ways of accepting an online offer? They should be, if the offer invites acceptance in this manner. As a general rule, contracts can be created and accepted by conduct, if reasonable under the circumstances.[10]

Contracts can be accepted by a nod of the head or shaking hands, sending or depositing a check, sending a purchase order, shipping goods, or the act of taking product off a shelf.[11] One can even accept a shrinkwrap license by opening the package, in some circumstances.[12]

Mere silence by itself will not create a contract.[13] However, the types of actions typically involved in online transactions—clicking and downloading—are more deliberate than mere silence, and, depending on the situation, they should be proper forms of acceptance.

Offers and Acceptances by Computers

Can the act of a *computer* (without human involvement) create a contract? The answer should be yes, again depending on the circumstances.

A computer can generate an offer. For example, an inventory system can calculate when supplies are low and automatically generate an electronic purchase order to the vendor. Would such an order be a binding offer? While there are not yet any cases directly on point, one case has upheld the validity of a computer generated insurance renewal.[14] The court, reasoning that the computer operates only in accordance with the information and directions supplied by its programmers, held the insurance company was bound by the computer-generated renewal notice.

Under pending draft revisions to the Uniform Commercial Code (UCC), computer-generated offers would be valid. Electronic messages could form a contract, even if not actually seen or reviewed by a human.[15]

Acceptances can also be generated by computer. However, they will be analyzed in the same way as their human-generated counterparts—is the message an acceptance or merely an acknowledgment of receipt? In most cases it will depend on the nature of response. For example, in a case involving a computer order entry system, orders were placed by Touch Tone phone, and the system automatically generated a tracking number for each order. When the seller refused to fill the buyer's order, the buyer sued. The court held that no contract had been created, since the tracking number was merely for administrative convenience and not a clear acceptance.[16]

This issue will certainly arise in EDI transactions, where a computer can automatically acknowledge receipt of an electronic purchase order. However, this type of acknowledgment usually only means the computer received the message in a form it could read.[17] It does not necessarily mean the order was accepted. However, other types of EDI messages, such as purchase order acknowledgments, would be proper acceptances.

Timing of Acceptances–The Mailbox Rule

Timing of acceptances can be important in determining if there is a binding contract. That is because a offer can generally be revoked if it has not yet been accepted.[18] What happens if the person who made the offer revokes it, but the other party's acceptance is already in the mail? Under the so-called "mailbox rule," there would be a contract. The acceptance would take effect as soon as it was out of the sender's control, if it was sent in a manner and by a medium invited by the offer.[19]

Will the mailbox rule be applied to electronic acceptances? It seems unlikely, although there are no cases on point.[20] The mailbox rule applies to mail and telegraph, but not to communications that are essentially instantaneous, such as telephone and telex.[21] Under pending draft revisions to the UCC, the mailbox rule would not apply to electronic communications.[22]

Timing can also be important when a contract sets a deadline for acceptance. For example, in one case, a fax transmission was not effective notice, because it was started before the deadline passed, but not completed until afterwards.[23] Electronic transmissions may pose similar problems, especially since there can be a delay between sending and receipt.

LEGAL REQUIREMENTS FOR ELECTRONIC CONTRACTS

Even if an offer and acceptance are present, more is required. For electronic contracts to be viable, from both a legal and a business perspective, the communications that are exchanged and the records that are preserved of these communications must satisfy certain legal requirements. While not all of these requirements will apply in every situation, they generally include the following:

- Authenticity
- Integrity
- Nonrepudiation
- Writing and signature

Authenticity

Authenticity is concerned with the source or origin of a communication.[24] Who is the message from? Is it genuine or a forgery?

A party entering into an online contract must be confident of the authenticity of the communications it receives. For example, when a bank receives an electronic payment order from a customer directing that money be paid to a third party, the bank needs to be able to verify the source of the request. The bank is faced with the problem of ensuring that it is not dealing with an impostor.[25]

Likewise, a party must also be able to establish the authenticity of its electronic transactions should there ever be a dispute. To accomplish this, that party must retain a record of all relevant communications pertaining to the transaction, and keep those records in such a way that it can show that the records are authentic. For example, if one party to a contract later disputes the nature of its obligations, the other party may need to prove the terms of the contact to a court. A court, however, will first require that the party establish the authenticity of the record it retained of that communication before the court will consider it as evidence in the case.[26]

Integrity

Integrity is concerned with the accuracy and completeness of the communication. Is the document the recipient received the same as the document that the sender sent? Is it complete? Has the document been altered either in transmission or storage?

The recipient of an electronic message needs to be confident of a communication's integrity before he will rely and act on it. Integrity is critical to electronic commerce when it comes to the negotiation and formation of contracts online, the licensing of digital content, and the making of electronic payments, as well as to proving up these transactions using electronic records of them at a later date. For example, a building contractor wants to be able to solicit bids from subcontractors and submit its proposal to the government online. The building contractor needs to be able to verify the accuracy of the bids upon which it will rely in formulating its proposal. The building contractor is faced with the problem of how to confirm that the bids as received are accurate.

Likewise, if the contractor ever needs to prove the amount of the subcontractor's bid, a court will first require that the contractor establish the integrity of the record he retained of that communication before the court will consider it as evidence in the case.[27] Even a communication that has been transmitted and received with its integrity intact may be accidentally or intentionally altered while in storage. Hardware that is not functioning properly or software with errors may alter the contents of an electronic record in the process of storing or retrieving it.

Nonrepudiation

Nonrepudiation is concerned with holding the sender to his communication. The sender should not be able to deny having sent the communication if he did, in fact, send it, or claim that the contents of the communication as received are not the same as what the sender sent if, in fact, they are what was sent. Nonrepudiation is essential to electronic commerce when it comes to a trading partner's willingness to rely on a communication, electronic contract, or funds transfer request. For example, a stockbroker who accepts buy/sell orders over the Internet would not want his client to be able to

A party must be able to establish the authenticity of its electronic transactions should there ever be a dispute.

The essence of the requirement is that the communication be reduced to a tangible form.

place an order for a volatile commodity, such as a pork bellies futures contract, and then be able to confirm the order if the market goes up and repudiate it if the market goes south.[28]

Nonrepudiation becomes a legal requirement when the relying party seeks to hold the other party to the deal. The relying party must be able to establish the fact that the other party agreed to the contract and the terms of their agreement.

Writing and Signature

In many cases, the law requires that an agreement be both (1) documented in "writing" and (2) "signed"[29] by the person who is sought to be held bound in order for that agreement to be enforceable. Contract law provides that contracts for the sale of goods for the price of $500 or more are not enforceable unless there is both a writing sufficient to indicate that a contract has been made between the parties, and that it is signed by the party against whom enforcement is sought.[30]

Numerous other statutes governing other forms of transactions also require that a transaction be documented by a writing and a signature. Certain statutes regarding corporate and partnership actions prescribe writing and signature requirements. For example, a new general partner may only be added to a partnership upon the written consent of all partners in some states.[31]

In addition, federal, state, and local governments also require that transactions be signed and in writing. For example, federal government contracts must be in writing and executed, or signed, before the government will consider itself bound.[32] Similarly, many municipal governments have adopted the Model Procurement Code, which mandates that the purchase of supplies and services in excess of $5,000 be by formal, written contract.[33]

For contracts formed online, the traditional form of a writing (paper) and the traditional handwritten signature do not exist. So how can online contracts meet these legal requirements?

The Writing Requirement. When the statute of frauds applies, there must be a writing sufficient to indicate that a contract has been made between the parties.[34] As discussed below, electronic transmissions recorded in a tangible form should meet the writing requirement.

The definition of a "writing" is not limited to ink on paper. Rather, the essence of the requirement is that the communication be reduced to a tangible form.[35] As early as 1869, a New Hampshire court found a telegraphed contract to be a sufficient writing under the statute of frauds, stating:

> [i]t makes no difference whether that operator writes the offer or the acceptance. . .with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by use of the finger resting upon the pen; not does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office.[36]

The courts have also found telexes, Western Union Mailgrams, and even tape recordings to be writings under the statute of frauds.[37] Faxes have been assumed (without express decision) to be writings under the statute of frauds.[38] Magnetic recordings of data on computer disks have been held to constitute "writings" for purposes other than the statute of frauds, including under forgery statutes and copyright law.[39]

Electronic transmissions recorded in a tangible medium should therefore be deemed to satisfy the writing requirement.[40]

The Signature Requirement. Generally, a signature is "any symbol executed or adopted by a party with present intention to authenticate a writing."[41] Thus, a signature need not be ink on paper—rather, the issue is what the signer intended.

The courts have found many symbols to be signatures under the statute of frauds: names on telegrams,[42] names on telexes,[43] typewritten names,[44] names on Western Union Mailgrams,[45] and even names on letterhead.[46] Faxed signatures have been assumed to constitute effective signatures, under non-statute of frauds cases.[47]

Thus, a symbol or code on an electronic record, intended as a signature, will likely meet the statute of frauds requirement.[48] Thus, even a

named typed at the end of an e-mail can be a signature,[49] so long as it was made with the proper intent. Digital signatures should also qualify. Both the ABA *Digital Signature Guidelines* and digital signature statutes enacted in several states provide that a digital signature will meet any legal requirement for a signature.[50]

DIGITAL COMMUNICATIONS AND SECURITY PROCEDURES

Digital information, by its very nature, is easily copied and altered. The risk is particularly great while it is passing through an open network or while it resides on a computer system beyond the sender's control. Moreover, when information is received over an open network (such as the Internet), there is often no assurance as to the source. Information or message level security can provide assurances that the digital information, although it can be accessed, is authentic and has not been modified, regardless of where it resides.

Information is protected through the use of a security procedure. A security procedure is a methodology or procedure used for the purpose of (1) verifying that an electronic record is that of a specific person or (2) detecting error or alteration in the communication, content, or storage of an electronic record since a specific point in time. A security procedure may require the use of algorithms or codes, identifying words or numbers, encryption, answer back or acknowledgment procedures, or similar security devices.[51]

In many cases, security procedures involve the implementation of sophisticated technology. But it is important to recognize that security procedures have legal significance. The first formal recognition of the legal effect of information security procedures occurred in 1989 with the approval of a UCC Article 4A.[52]

UCC Article 4A addresses the electronic transfer of funds by wire.[53] A person who wishes to transfer funds electronically does so by transmitting an electronic message, called a payment order, to his bank. Because that message cannot bear a traditional handwritten signature or other paper-based security measure, information security measures must be used instead. The UCC recognized this and the reality that a bank receiving a payment order needs something objective on which it can rely in determining whether it may safely act on that order.[54]

Article 4A modernized the law by providing that a bank could rely on information security procedures as a substitute for the traditional time-tested requirement of a signature. Under Article 4A, an electronic message instructing a bank to transfer funds to a payee is considered valid, and the bank is authorized to transfer the funds in accordance with the order if (1) the bank's customer actually authorized the order or (2) if the authenticity and integrity of the order is "verified" pursuant to a "commercially reasonable" security procedure regardless of whether the order was actually authorized by that person.

The bottom line is that Article 4A adopts "security procedures" rather than "signatures" as the basis for verifying transactions and apportioning liability. This establishes an important precedent.

An important precedent: Article 4A adopts "security procedures" rather than "signatures" as the basis for verifying transactions and apportioning liability.

USING DIGITAL SIGNATURES

Digital signatures are one of the most promising information security measures available to satisfy the legal and business requirements of authenticity, integrity, nonrepudiability, and writing and signature. Unlike handwritten signatures, they are created using public key encryption.

What Is a Digital Signature?

A *digital signature* is an electronic substitute for a manual signature that serves the same functions as a manual signature and more. It is an identifier created by a computer instead of a pen. Technically, a digital signature is the sequence of bits that is created by running an electronic communication through a one-way hash function and then encrypting the resulting message digest with the sender's private key.[55] It is an unintelligible string of alphanumeric characters, such as the following:

A digital signature is derived from the document to be digitally signed. Any change to the document will produce a different digital signature.

owHtWX1sU1UUP+91G+22ysbHhDHcBeZ
AVmq7L9iAuNJ2UuhX2soUSpaufVsftu8tby1
kUXTGsGhAgsEY4h9b+EPBgArBGNSEL
GpiNEFM5A80xIzEoPiPSEiMRFbPfR/ajW
7rlBjR/ZbfO/eed9+599177j3ndS9CWlcIlqe3
Df1w45vqJ85+dZ5hPkywt6uOjb5zYvRmy2dr
FnZKT17a/97n/Tt11d8dNmyvqVl2K7jt8Lxf
Vr9We2jHyk

As the foregoing makes clear, a digital signature is not anything like a handwritten signature. A digital signature is not a digitized image of a handwritten signature or a typed signature such as "/s/john doe." Moreover, unlike a handwritten signature, which is unique to the signer, but presumably consistent across all documents signed, a digital signature is unique for each document signed. This is because a digital signature is derived from the document to be digitally signed. Any change to the document will produce a different digital signature.

A digital signature can serve the same purpose as a handwritten signature in that it may signify authorship, acknowledgment, or assent, among other things. However, a digital signature also serves important information security purposes that handwritten signatures cannot. A digital signature allows the recipient of a digitally signed communication to determine whether the communication was created by the purported signer and whether it was changed since it was digitally signed. That is, a digital signature provides assurance as to the authenticity, nonrepudiability, and integrity of the communication. Because a digital signature provides these security assurances, it is to this extent superior to a handwritten signature.

How Is an Electronic Communication Digitally Signed?

Before a sender can digitally sign an electronic communication, the sender must first generate a public-private key pair. The private key (a large prime number) is kept confidential by the sender and is used for the purpose of creating digital signatures. The public key (another large, but related, prime number) can be disclosed generally by posting the key in online databases, repositories, or anywhere else the recipient of the digitally signed message can access it.

To digitally sign an electronic communication, the sender runs a computer program that creates a unique message digest (or hash value) of the communication. The program then encrypts the resulting message digest using the sender's private key. The encrypted message digest is the digital signature.[56] The sender then attaches the digital signature to the communication and sends both to the intended recipient. A digitally signed communication looks like this:

October 30, 1998

Dear Order Department:

We commit to purchase 10,000 widgets at your price of $175 per hundred.

Ship to:

Industrial Products Co.
555 Retail Drive
Chicago, Illinois 60061

Sincerely,
Purchasing Department,
Industrial Products Co.

——BEGIN SIGNATURE——

owHtWX1sU1UUP+91G+22ysbHhDHc
BeZAVmq7L9iAuNJ2UuhX2soUSpaufVs
ftu8tby1kUXTGsGhAgsEY4h9b+EPBgA
rBGNSELGpiNEFM5A80xIzEoPiPSEi
MRFbPfR/ajW7rlBjR/ZbfO/eed9+59917
7j3ndS9CWlcIlqe3Df1w45vqJ85+dZ5hP
kywt6uOjb5zYvRmy2drFnZKT17a/97n/
Tt11d8dNmyvqVl2K7jt8LxfVr9We2jHyk

——END SIGNATURE——

The digital signature process can be made very easy. With a user-friendly software interface, the user may complete the signature process by using a mouse to click on applicable buttons. No special technical expertise is needed to digitally sign a document. The end user should, however, appreciate the legal effects and consequences of digitally signing an electronic communication.

Verifying a Digital Signature

When a recipient gets a digitally signed communication, the recipient's computer runs a computer program containing the same cryptographic algorithm and hash function the sender used to create the digital signature. The program

automatically decrypts the digital signature (the encrypted message digest) using the sender's public key. If the program is able to decrypt the digital signature, the recipient knows that the communication came from the purported sender, that is, the recipient has verified its authenticity. This is because only the sender's public key will decrypt a digital signature encrypted with the sender's private key.

The program then creates a second message digest of the communication and compares the decrypted message digest with the digest the recipient created. If the two message digests match, the recipient knows that the communication has not been altered or tampered with, that is, the recipient has verified its integrity.

Prerequisites for Use of Digital Signatures

The effectiveness of the digital signature process depends upon the reliable association of a public-private key pair with an identified person. The discussion thus far has made one critical assumption. That is, that the public-private key pair of the sender does, in fact, belong to the sender. Any assurance of authenticity/nonrepudiability would be worthless if the public key used to decrypt a digital signature belonged to an impostor and not the named sender.

Paper signatures usually have an intrinsic association with a particular person because they consist of that person's unique handwriting. However, public-private key pairs used to create digital signatures have no intrinsic association with anyone because private and public keys are nothing more than large numbers. When a recipient obtains the public key of someone from whom he has received a digitally signed communication, how does he know that the public key does, in fact, belong to the sender? An impostor could have generated the public-private key pair and entered his public key in a public database under the recipient's name.

The solution to this problem is to enlist a third party trusted by both the sender and recipient with performing the tasks necessary to associate a person or entity on one end of the transaction with the key pair used to create the digital signature on the other. Such a trusted third party is called a *certification authority.*

Only the sender's public key will decrypt a digital signature encrypted with the sender's private key.

CERTIFICATION AUTHORITIES

A certification authority (CA) is a trusted third person or entity that ascertains that a certain public key corresponds to a private key and that the public key belongs to an identified person.[57] The certification process generally works in the following way. The user:

1. generates her own public/private key pair;
2. contacts the CA (either in person or online) and produces proof of identity, such as a driver's license and passport or any other proof required by the CA; and
3. demonstrates that he or she holds the private key corresponding to the public key (without disclosing the private key).

Once the certification authority has verified the association between an identified person and a public key, the certification authority then issues[58] a certificate. A certificate is a computer-based record that attests to the connection of a public key to an identified person or entity.[59] A certificate identifies the certification authority issuing it and the person (called a subscriber) identified with the public key. The certificate also contains the subscriber's public key and possibly other information, such as an expiration date for the public key.[60] To provide assurance as to the authenticity and integrity of the certificate, the certification authority attaches its own digital signature to the certificate.

Who Can Be a Certification Authority?

In theory, anyone can be a certification authority. This includes federal and state governmental entities, and private persons or entities acting as certification authorities for commercial purposes. For example, the U.S. Postal Service has considered offering services designed to facilitate electronic commerce, including functioning as an all-purpose

Through its nationwide network of post offices, the USPS can register public keys for applicants who appear in person.

There are also a number of private commercial certification authorities.

certification authority. The USPS may be well-suited to function as a CA: In transactions between companies or individuals, it is an objective third party with an established reputation for credibility.

Through its nationwide network of post offices, the USPS can register public keys for applicants who appear in person. This will enable USPS to provide an added level of security, such as photographs and fingerprinting, to ensure that each registered public key corresponds to a real person, not an alias or assumed identity.

There are also a number of private commercial certification authorities. These include VeriSign Inc., which issues certificates and provides related services to corporations and individuals for use in digitally signing documents for any purpose,[61] and GTE.[62]

OBLIGATIONS OF THE PARTIES

There are typically three parties to a digitally signed electronic communication: the sender of the message (who digitally signs the message), the recipient of the message, and the certification authority who issues the certificate used by the recipient to verify the digital signature. The obligations and responsibilities of each of these three parties have been the source of extensive debate and, in several cases, the subject of legislation.

The following summary of the obligations of the various parties is based on the analysis of these issues set forth in the American Bar Association *Digital Signature Guidelines,* and the statutory approach to these issues taken in the Utah Digital Signature Act. However, it is important to understand that there is not yet universal agreement with respect to these issues.

Signer

When a party to an electronic transaction uses a digital signature, that party undertakes certain obligations and makes certain representations. First, a party digitally signing a document has an obligation to do so using a private key that was generated using a trustworthy system.[63] A trustworthy system consists of hardware, software, and procedures that

(1) are reasonably secure from intrusion and misuse;

(2) provide a reasonable level of availability, reliability, and correct operation; and

(3) are reasonably suited to performing their intended functions.[64]

Trustworthiness is in part a question of security. It requires, among other things, the use of system security measures such as access controls, division of duties among personnel (so that a single employer could not compromise key pairs or the system without colluding with another employee), and audit procedures. Security measures need only be reasonable, not absolute, under the circumstances.[65]

To the extent that the public key used to verify a digital signature is the subject of a certificate issued by a certification authority, the signer has an obligation to see that all representations made to the certification authority for inclusion in the certificate or use in generating the certificate are accurate to the best of the signer's knowledge and belief.[66] If any information is false or misleading—or becomes so as a result of future events—the signer has an obligation to notify the certification authority so that it may be corrected.[67]

If a third party relies on this false information and is damaged as a result, the signer may be liable to both the relying party and the certification authority.[68] Because of this potential liability, a signer is given an opportunity to review and accept a certificate before it is published.[69]

A signer must retain control of the private key, protect it from being compromised, and keep it secret.[70] A signer may lose control over the key by voluntarily disclosing it to someone not authorized to sign on the signer's behalf, by losing the disk, Smartcard, or other object on which the key is stored, or by theft. If the signer loses control over the key, the signer may be held liable for any obligations or bills incurred by an

unauthorized user.[71] A failure to safeguard the private key can have serious consequences.

A signer may limit his exposure by requesting that the certification authority suspend or revoke his certificate as soon as the signer learns the key has been compromised. Because a certification authority will generally have no duty or ability to monitor either the continuing accuracy of information in the certificate or events (such as loss of a key) that may warrant suspension or revocation, the signer has an obligation to request that the certificate be suspended or revoked (and to stop using the private key to create digital signatures).[72]

A signer also has an obligation to make the corresponding certificate available to the recipient of the communication if the signer expects the recipient to rely on the digital signature. The signer may make the certificate available by publishing it in a repository maintained by the certification authority or a public repository or by attaching the certificate to the communication itself.

Certification Authority

A certification authority's primary function is to issue a certificate that verifies the relationship between a public key and a person or entity. It is a given that third parties will rely on certificates it issues to verify digital signatures.[73] Accordingly, a certification authority has some level of obligation to verify (1) the identity of the person to whom it issues a certificate and (2) that the public key listed in the certificate corresponds to a private key held by that person.[74] Otherwise, a recipient of a digital signature who is misled by a certificate into relying on a digital signature may have a claim against the certification authority for misrepresentation.

The amount of investigation a certification authority will undertake may vary according to the purposes for which the digital signature and certificate are to be used.[75] The amount of investigation may be specified by the certification authority in its certification practice statement or by contract between the certification authority and subscriber.[76] State statutes may establish minimum requirements.[77]

In order to limit the certification authority's liability stemming from representations attributed to them by the act of issuing a certificate, a certificate will normally include an expiration date.[78] This helps eliminate liability for claims of reliance on stale information. Upon expiration of a certificate, the certification authority no longer makes any representations as to the expired certificate and is discharged of its duties.[79] A person who relies on an expired certificate and is damaged will have no claim against the certification authority because it was not reasonable to have relied on the expired certificate.[80]

In addition, certification authorities may also include in a certificate other forms of limitations of their liability, such as dollar limits, which are sometimes referred to as *reliance limits.*[81] A reliance limit is a warning that certificates the CA issues should not be relied on for transactions in excess of a specified dollar amount. Such a reliance limit may also be specified in a certification practice statement or set by a licensing body as a limit on a certification authority's license to issue certificates.[82] If a third party who knows of the reliance limit relies on a digital signature in connection with a transaction that exceeds the limit, that third party may not be able to recover its losses from the certification authority because it was not reasonable to so rely.

Because of the importance of certificates in electronic commerce, a certification authority must promptly revoke a certificate at the request of the person named in the certificate.[83] Just like canceling a stolen credit card, revoking a certificate is necessary to put potential relying parties on notice that messages digitally signed with a person's private key may no longer be reliable. With revocation requests, however, the certification authority must confirm the identity of the person making the request.[84] If the subscriber has digitally signed a large number of documents, improperly revoking a certificate could cause monumental problems.

A certification authority must promptly revoke a certificate at the request of the person named in the certificate.

Several states have recognized the need to provide the legal infrastructure to support the use of digital signatures.

Relying Party

A recipient of a digitally signed communication, or other *relying party,* does not have prescribed obligations or duties as such. A relying party, for instance, has no duty to examine a certificate to determine whether a key is expired or not. Nor does a relying party have a duty to check a certification reliance limit to determine whether a certificate has been suspended or revoked. However, if a relying party fails to do these things or to otherwise verify the signature, the relying party assumes the risk that the digital signature is a fake and the relying party's recourse may be limited.[85]

LEGAL EFFECT OF A DIGITAL SIGNATURE

Although there is no generally accepted, uniform law on the subject, several states have recognized the need to provide the legal infrastructure to support the use of digital signatures. Utah was the first to pass digital signature legislation.[86] Utah's Digital Signature Act establishes a scheme of optional licensure[87] and regulation[88] for private companies, individuals, and governmental bodies wishing to act as certification authorities.

The legislation establishes minimum standards that certification authorities must meet to be licensed.[89] These standards include minimum procedures that a certification authority must follow in issuing a certificate.[90] The legislation accords to a digitally signed communication—one that has been certified by a licensed certification authority—certain legal presumptions and effects that a communication certified by a nonlicensed certification authority does not receive, such as that the communication satisfies writing and signature requirements and was signed by the subscriber with the intention of signing the message.[91] The Utah act also addresses the respective duties and liabilities of licensed certification authorities,[92] subscribers,[93] and repositories.[94]

California has also enacted digital signature legislation.[95] California's legislation as originally introduced was very similar to Utah's. The statute that was enacted takes a more limited approach in that it applies only to communications with public entities, whereas the Utah statute applies to anyone who wishes to use digital signatures.[96]

A more comprehensive effort to address the legal effect of a digital signature has been undertaken by the Information Security Committee of the American Bar Association's Electronic Commerce Division, which formulated the *Digital Signature Guidelines.*[97] Based on these early efforts, it appears that certain legal conclusions can be drawn about the likely legal effect of using digital signatures.

Integrity

Digital signatures provide a means to verify the integrity of an electronic communication. Generally, if a digital signature can be properly verified through the use of the corresponding public key, then it will be presumed that the message has not been altered since the digital signature was created.[98]

Authenticity

Digital signatures also verify the source of an electronic communication. The recipient knows that the communication is authentic (in that it came from the sender) because only the sender's public key will decrypt a digital signature encrypted with the sender's private key. Because the public and private keys are associated with an identified signer and are unique to each signer, the key effectively links the signer to the document.[99]

Thus, if a digital signature can be verified through the use of the sender's public key, it will be presumed that the digital signature was created by the private key corresponding to the public key, and that the digital signature was affixed with the intention of the sender to identify himself as the source of the communication.[100]

Nonrepudiation

When the authenticity and integrity of a communication can be established, the sender is prevented from repudiating the contents of the communication or having sent it. The digital

signature cannot be forged unless the sender lost control of his private key. The recipient cannot forge a document to himself, either. Even if the recipient were to create a digital signature using the sender's public key, the digital signature can only be decrypted using the sender's private key. The same key cannot encrypt and decrypt a single communication.

Writing and Signature Requirements

Like paper documents, electronic documents are governed by rules (such as the statute of frauds) that require certain documents to be "in writing" and "signed." The general view is that the use of a digital signature will satisfy the signature[101] and any writing requirement.[102]

Right to Rely

If a digital signature can be verified by the recipient, the recipient is entitled to rely generally on the communication, and the sender (the person digitally signing the message) will be bound.[103] However, if the digital signature cannot be verified, the recipient is not required to rely on it for identification of the purported sender and may not be justified in doing so.[104]

New Paradigm Shift

With handwritten signatures, the law provides that a person is not liable for forgeries or other unauthorized signatures.[105] With digital signatures, especially under some of the new and proposed legislation, a person may be liable for messages signed with his private key until he revokes his certificate.[106] In such a case, a person who holds a public-private key pair has an increased responsibility similar to that of a person who signs documents using a signature machine. The person with the machine may not be able to challenge an unauthorized machine-made signature if that person has been negligent in keeping the machine secure. The signer must understand that he may be bound by any communication digitally signed with the private key that corresponds to the public key, and will be held liable to anyone who relies on the public key before the key was revoked and is damaged.

The result is similar to that in the electronic payments context, in which a person who has agreed that a bank may honor a payment order that the bank has verified through the use of commercially reasonable security procedures will bear the loss for a payment that was not in fact authorized. If this potential liability is not enough to cause a person to safeguard his private key, the law may impose an affirmative duty on the person to do so.[107]

The author's biography may be found on page 39.

Like paper documents, electronic documents are governed by rules that require certain documents to be "in writing" and "signed."

Endnotes

[1] Adapted from Thomas J. Smedinghoff, *Online Law* (Addison-Wesley, 1996).

[2] See *Corinthian Pharmaceutical Systems v. Lederle Labs,* 724 F. Supp. 605 (S.D. Ind. 1989); *Electronic Marketplace,* Electronic Com. Bull 8 (Oct. 1992); *Fax Pump Melds Fax, Call Processing Capabilities*, Network World, May 27, 1991, at 29, col. 2.

[3] See *On-Line Service to Assist Global Trade,* Wall St. Journal, Sept. 26, 1995 at B10 611 (AT&T, Dun & Bradstreet and others forming joint venture for a virtual business agency).

[4] UCC 2-204.

[5] Of course, there can be questions about the reliability of electronic communications, which may make it more difficult to introduce evidence in court. Information security matters are discussed below.

[6] UCC 2-206(1)(a).

[7] It is well established that an acceptance may properly be sent by the same means as the offer, unless the offer says otherwise. See *Restatement (Second) of Contracts* § 65.

[8] See e.g. *Market Development Corp. v. Flame-Glo Ltd.,* 1990 WL 116319 (E.D. Pa. 1990) (a mailed offer may be accepted by fax).

[9] For example, if the parties have regularly corresponded in the past by e-mail, an e-mail acceptance will probably be effective. However, in some cases a person may have an e-mail address which he rarely uses or does not monitor. In that case, it may not be appropriate to e-mail an acceptance to that person.

[10] UCC 2-203.

[11] *Cargill, Inc. v. Wilson,* 16 U.C.C. Rep. Serv. 615 (Mont. 1975) (sending check); *Mead Corp. v. McNally-Pittsburg Mfg. Corp.*, 654 F.2d 1197 (6th Cir. 1981) (sending purchase order); *Dubrofsky v. Messer,* 31 U.C.C. Rep. Serv. 907 (Mass. App. Div. 1981) (shipping goods); *Fender v. Colonial Stores, Inc.,* 19 U.C.C. Rep. Serv. 402 (Ga. App. 1976) (taking product off shelf).

[12] *ProCD v. Zeidenberg,* 86 F.3d 1447 (7th Cir. 1996); Arizona Retail Systems, Inc. v. The Software Link, Inc., 831 F. Supp. 759 (D. Ariz. 1993) (where no prior contract existed, opening a software package can constitute acceptance of terms on outside of package).

[13] *South Hampton Co. v. Stinnes Corp.,* 733 F.2d 1108 (5th Cir. 1984). In some cases a merchant's silence may constitute acceptance of additional terms to a contract, or may act to confirm a written summary of a verbal contract. *See* UCC 2-207, 2-201(2).

[14] *State Farm Mutual Auto. Ins. Co. v. Brockhurst,* 453 F.2d 533 (10th Cir. 1972)

[15] UCC 2B Section 204 (April 15, 1998 draft).

[16] *Corinthian Pharmaceutical Systems v. Lederle Labs,* 724 F. Supp. 605 (S.D. Ind. 1989). The seller's other correspondence stated that orders were not effective unless accepted by the seller.

[17] An EDI "functional acknowledgment" confirms that the message was functionally complete—that is, all fields in the form were completed with recognizable codes. It does not reflect acceptance of the substantive terms.

[18] However, "firm offers" may not be revoked early. A firm offer is one that is in writing and is specified as remaining open for a certain time. The offer may not be revoked before the time stated. See UCC 2-205 (relating to offers by merchants).

[19] *Restatement (Second) of Contracts* § 63. An offeror can avoid the mailbox rule by stating that acceptances will only be effective upon receipt. Id.

[20] A British case has apparently applied a mailbox rule for a litigation deadline. There, a court document was entered into an e-mail system at a police station before the deadline, but not printed out in court until afterwards. The court held the deadline was met. *The London Times,* July 28, 1988 at 27, Col. 1 (1988) C.L.Y. 664. However, it is one thing to hold that a filing meets a court deadline, and another to hold a party is bound to a offer which it in good faith canceled.

[21] *Restatement (Second) of Contracts* § 64. Although electronic messages are transmitted very quickly, they are not instantaneous. In many systems, messages are routed through networks and administrators and can be delayed for a matter of hours or even days.

[22] UCC Art. 2B–120 (April 15, 1998 draft). Also See Raymond T. Nimmer, *Electronic Contracting, Legal Issues* (Paper presented at the American Bar Association Science and Technology Section Meeting, 8/6/95). The ABA model for EDI trading partner agents also rejects the mailbox rule. Electronic Messaging Services Task Force, *The Commercial Use of Electronic Data Interchange—A Report,* 45 Bus. Law 1647 (1990).

[23] *Bomen Inc.,* Comp Gen B-234652, May 17, 1989, 3 CGEN (CCH) ¶ 103,198 (1989) (23-page fax started, but not completed, before the deadline).

[24] See Fed. R. Evid. 901(a) (1995).

[25] See U.C.C. 4A-202, 4A-203 & Official Comment. Section 4A-202 solves this problem for a bank and its customer who has agreed to transact its banking electronically and to be subject to Article 4A. If the bank verifies the payment order through the use of a commercially reasonable security procedure, the customer will be bound even if it did not in fact authorize the payment order. U.C.C. 4A-202(b). If, however, the customer can prove that the person sending the fraudulent payment order did not obtain the information necessary to send such order from an agent or a source controlled by the customer, the loss is shifted back to the bank. U.C.C. 4A-203(a)(2). If the bank does not follow the security procedure and the order is fraudulent, the bank will generally have to cover the loss. U.C.C. 4A-202(a).

[26] See, e.g., *U.S. v. Eisenberg,* 807 F.2d 1146 (8th Cir. 1986) (authenticity of a letter disputed); *U.S. v. Grande,* 620 F.2d 1026 (4th Cir.) (authenticity of invoice disputed), *cert. denied*, 449 U.S. 830, 449 U.S. 919 (1980).

[27] See, e.g., *Victory Med. Hosp. v. Rice,* 143 Ill. App. 3d 621, 493 N.E.2d 117 (1986).

[28] See, generally, "Follow the Money—A New Stock Market Arises on the Internet," Scientific American 31 (Jul. 1995).

[29] The Uniform Commercial Code (UCC) defines "signed" as "any symbol executed or adopted by a party with present intention to authenticate a writing." U.C.C. 1-201 (39)(1991).

[30] U.C.C. 2-201(1) (1991). *See also* U.C.C. 1-206 (1991)(limiting enforcement of unsigned, unwritten contracts for the sale of securities for $5,000 or more). For a state-by-state listing of state statutes of frauds, see *Restatement (Second) of Contracts,* § 110 statutory note, at 284-85 (1982).

[31] Uniform Limited Partnership Act § 401 (1976).

[32] See Pub. L. No. 97-258, 96 Stat. 927 (1982)(codified at 31 U.S.C. § 1501). Federal courts also require all documents to be filed to be signed. *See* Fed. R. Civ. Proc. 11 (1995).

[33] Model Procurement Code For State and Local Governments § 3-204.

[34] See UCC 2-201. There is a great deal of case law regarding how detailed the signed writing must be. Those issues will be no different for online contracts. For example, in one case, a handwritten (unsigned) memo, plus signed payroll cards, were together deemed to be a sufficient signed writing to evidence a contract. *Crabtree & Evelyn v. Elizabeth Arden Sales Corp.*, 305 N.Y. 48, 110 N.E.2d 551 (1953).

[35] UCC 1-201(46) defines "written" or "writing" as "printing, typewriting or any other intentional reduction to tangible form."

[36] *Howley v. Whipple,* 48 N.H. 487 (1869). One commentator has noted that "the Whipple opinion was a bit eccentric in its metaphors, to be sure, but was not maverick in its results." *Note, The Statute of Frauds Online: Can a Computer Sign a Contract for the Sale of Goods?* 14 Geo. Mason U. L. Rev. 637 (Summer 1992).

[37] *Joseph Denunzio Fruit Co. v. Crane,* 70 F. Supp. 117 (S.D. Cal. 1948)(telex is a writing); *McMillan Ltd. v. Weimer Drilling & Eng. Co.,* 512 So.2d 14 (Ala. 1986) (mailgram is a writing); (*Ellis Canning Co. v. Bernstein,* 348 F. Supp. 1212 (D. Colo. 1972) (tape recording is a writing). *But see Roos v. Aloi,* 127 Misc. 2d 864, 487 N.Y.S.2d 637 (Sup. Ct. 1985) (tape recording is not a writing).

[38] See *Bazak International Corp. v. Mast Industries, Inc.,* 73 N.Y.2d 113, 7 U.C.C. Rep. 2d 1380 (1989) (faxes assumed without discussion to be writings under UCC 2-201). In *American Multimedia Inc. v. Dalton Packaging, Inc.,* 143 Misc. 2d 295, 540 N.Y.S.2d 410 (Sup. Ct. 1989), a faxed purchase order was assumed to be a writing for purposes of a federal arbitration statute.

[39] *People v. Avila*, 770 P.2d 1330 (Colo. Ct. App. 1988) (recording on computer disk was a "writing" for purposes of the forgery statute). See also *Clyburn v. Allstate,* 826 F.Supp. 955 (D.S.C. 1993). [Reference Copyright Act.].

[40] Some courts may have concerns about reliability—whether magnetic media are more subject to tampering than paper. However, these concerns should not affect whether or not an electronic transmission is considered a writing. Rather, they should only be relevant to the authentication, for evidence purposes, of a particular transmission record. *But see Note, The Statute of Frauds Online: Can a Computer Sign a Contract for the Sale of Goods?* 14 Geo. Mason U. L. Rev. 637 (Summer 1992) (author analyzes reliability of EDI records in determining whether to consider them "writings" under the statute of frauds).

[41] UCC 1-201(39).

[42] *Selma Savings Bank v. Webster County Bank,* 206 S.W. 870 (Ky. 1918); *Hillstrom v. Gosnay*, 188 Mont. 388 (614 P.2d 466 (1989). *Contra, Pike Industries, Inc. v. Middlebury Associates,* 398 A.2d 280 (Vt. 1979); *aff'd on other grounds,* 436 A.2d 725 (Vt. 1980), *cert denied,* 455 U.S. 947 (1992). *See Note, The Statute of Frauds Online: Can a Computer Sign a Contract for the Sale of Goods?* 14 Geo. Mason U. L. Rev. 637 (Summer 1992).

[43] *Joseph Denunzio Fruit Co. v. Crane,* 70 F. Supp. 117 (S.D.Cal. 1948); *Franklin County Coop. v. MFC Services,* 441 So.2d 1376 (Miss. 1983); *Hideca Petroleum Corp v. Tampimac Oil Int'l Ltd.,* 740 S.W.2d 838 (Tex. Ct. App. 1987). *But see Miller v. Wells Fargo Bank International Corp.,* 406 F. Supp. 452 (S.D.N.Y. 1975) (court suggested that there was a question as to whether test key on telex is a signature).

[44] *In Watson v. Tom Growney Equip. Inc.,* 721 P.2d 1302 (N.M. 1986), a name typed on a purchase order was found to be a sufficient signature, since the signatory had deliberately filled out other details on the form. A typewritten signature on a UCC financing statement was found to satisfy the signature requirement of the statute of frauds in *Matter of Save On Carpet of Arizona, Inc.,* 545 F.2d 1239 (9th Cir. 1976), but not in *In re Carlstrom,* 3 UCC Rep. Serv. 766 (Bk. D. Me. 1966). *A & G Const. Co. v. Reid Bros. Logging Co.,* 547 P.2d 1207 (Alaska 1976) (typed name sufficient).

[45] *Hesenthaler v. Farzin,* 388 Pa. Super 37 (1989) (focus on intent to authenticate); *McMillan Ltd v. Warrior Drilling & Eng Co.,* 512 So. 2d 14 (Ala. 1986).

[46] In *Kohlmeyer & Co. v. Bowen,* 126 Ga. App. 700, 192 S.E.2d 400 (1972), a securities brokerage firm's name was printed on a confirmation statement for the sale of securities. The court found the printed name was intended as authentication, and met the signature requirement under the statute of frauds. Also see *Associated Hardware Supply Co. v. Big Wheel Distrib. Co.,* 355 F.2d 114 (3d Cir. 1966) (letterhead).

[47] In *Beatty v. First Exploration Fund 1987 and Co. Limited Partnership,* 25 B.C.L.R.2d 377 (1988), a British Columbia case, faxed signatures on proxy documents were sufficient to meet the signature requirements under a limited partnership agreement. In *Gilmore v. Lujan,* 947 F.2d 1340 (9th Cir. 1991), the court upheld an agency's determination that a fax did not meet the regulation's strict requirement that a document be "holographically signed in ink," but criticized the agency for its narrow-minded approach. In *Madden v. Hegadon,* 565 A.2d 725 (N.J. Super. 1989), aff'd 571 A.2d 296 (N.J. 1989), a fax signature was deemed effective for filing a nomination petition.

[48] See Wright, *The Law of Electronic Commerce,* 1994 Suppl. 102 (1994); *Lowry, Does Computer Stored Data Constitute a Writing for the Statute of Frauds and the Statute of Wills?* 9 Rutgers Computer & Tech. L.J. 93 (1982). However, some commentators have noted the

difference between electronic communications and more conventional means such as telegraph and telex, and that there should be some requirement to evidence a connection between the signature and the signatory. One commentator proposes that such a connection could exist if it were shown that the electronic communications system uses commercially reasonable security measures. Baum, *Analysis of Legal Aspects in EDI and the Law* 129 (1989).

[49] See Wright, *The Law of Electronic Commerce,* 1994 Suppl. 102 (1994).

[50] See, for example, § 46-3-401 of Utah Digital Signature Act.

[51] See UCC 4A,-201; Illinois Electronic Commerce Security Act, 1997 Ill. H.B. 3180, at Section 5-105.

[52] See U.C.C. 4A, Funds Transfers (1989). Article 4A has been adopted in all states.

[53] U.C.C. Prefatory Note (1990).

[54] U.C.C. § 4A-203 Official Comment.

[55] See Utah Code Ann. § 46-3-103(10) (1996); *Digital Signature Guidelines* § 1.11 (August 1, 1996); William Stallings, *Protect Your Privacy: A Guide for PGP Users* 20 (1995).

[56] *Digital Signature Guidelines* § 1.11.

[57] *Digital Signature Guidelines* § 1.6.

[58] *Digital Signature Guidelines* § 1.16.

[59] *Digital Signature Guidelines* § 1.5.

[60] *Digital Signature Guidelines* § 1.5.

[61] For more information about VeriSign's certification authority services, see http://www.verisign.com.

[62] For more information about GTE's certification authority services, see http://www.cybertrust.com.

[63] *Digital Signature Guidelines* § 4.1.

[64] *Digital Signature Guidelines* § 1.35.

[65] *Digital Signature Guidelines* § 1.35; Comments 1.35.2, 1.35.3.

[66] See Utah Code Ann. § 46-3-304; *Digital Signature Guidelines* § 4.2.

[67] *Digital Signature Guidelines* § 4.2 Comment 4.2.1.

[68] Utah Code Ann. § 46-3-304; *Digital Signature Guidelines* § 4.2 Comment 4.2.2, 4.2.3.

[69] Utah Code Ann. § 46-3-304; *Digital Signature Guidelines* § 4.2 Comment 4.2.4.

[70] Utah Code Ann. § 46-3-305(subscriber has duty to exercise reasonable care to control private key); Cal. Gov't Code § 16.5(a)(3); *Digital Signature Guidelines* § 4.3.

[71] U.C.C. 4A-202(b); Utah Code Ann. § 46-3-302(1)(a).

[72] *Digital Signature Guidelines* § 4.4.

[73] *Digital Signature Guidelines* § 2.3 and Comment 2.3.1.

[74] Utah Code Ann. § 46-3-302; *Digital Signature Guidelines* § 3.7 & Comment 3.7.1.

[75] *Digital Signature Guidelines* § 3.7 Comment 3.7.1.

[76] *Digital Signature Guidelines* § 3.7 Comment 3.7.2.

[77] See Utah Code Ann.§ 46-3-304(3).

[78] See Utah Code Ann. § 46-3-308; Digital Signature Guidelines § 1.22.

[79] Utah Code Ann. § 46-3-308.

[80] See *Digital Signature Guidelines* § 5.4.

[81] See Utah Code Ann. § 46-3-309 (1995); *Digital Signature Guidelines* § 3.3 Comment 3.3.1.

[82] See Utah Code Ann. § 46-3-309; *Digital Signature Guidelines* § 3.3 Comment 3.3.1.

[83] Utah Code Ann. § 46-3-306-307; *Digital Signature Guidelines* § 3.10.

[84] See Utah Code Ann. § 46-3-307(1); *Digital Signature Guidelines* § 3.10.

[85] See *Digital Signature Guidelines* § 5.3.

[86] Utah Code Ann. § 46-3-101 to -504 (enacted Mar. 9, 1995; amended in 1996).

[87] See Utah Code Ann. § 46-3-201 (1996).

[88] Utah Code Ann. § 46-3-202 to -204, 46-3-301 to -310 (1996).

[89] Utah Code Ann. § 46-3-201 (1996).

[90] See Utah Code Ann. § 46-3-302 (1996).

[91] Utah Code Ann. § 46-3-401 to -406 (1996).

[92] Utah Code Ann. § 46-3-301 to -310 (1996).

[93] Id.

[94] Utah Code Ann. § 46-3-501 to -502 (1996).

[95] Cal. Gov't Code § 16.5.

[96] See Cal. Gov't Code § 16.5(a).

[97] *Digital Signature Guidelines* § 1.1-5.6 (August 1, 1996).

[98] Utah Code Ann. § 46-3-103(39), 46-3-406(3); *Digital Signature Guidelines* § 1.33, 5.6(2); cf. Cal. Gov't Code § 16.5(a)(4).

[99] *Digital Signature Guidelines* § 111.

[100] See Utah Code Ann. § 46-3-406(3); Cal. Gov't Code § 16.5; *Digital Signature Guidelines* § 5.6.

[101] See Utah Code Ann. § 46-3-406(3) (use of digital signature creates a presumption that document was signed with an intent to authenticate the document; Cal. Gov't Code § 16.5 (digital signature has same force and effect as manual signature); *Digital Signature Guidelines* § 5.2 & Comment 5.2.1; *see also* U.C.C. 4A-202(b); National Conference of Commissioners on Uniform State Laws, Uniform Commercial Code Revised Article 2. Sales. § 2-102(37) (draft Oct. 1, 1995)[hereinafter Revised U.C.C.].

[102] See Utah Code Ann. § 46-3-403 (1996); Digital Signature Guidelines § 5.1 & Comment 5.1.1.

[103] See Utah Code Ann. § 46-3-406(3); *Digital Signature Guidelines* § 5.6; see also U.C.C. 4A-202; Revised U.C.C. 2-212.

[104] See *Digital Signature Guidelines* § 5.3.

[105] See U.C.C. § 3-404.

[106] See Utah Code Ann. § 46-3-306(5); *Digital Signature Guidelines* § 5.6(1).

[107] See Utah Code Ann. § 46-3-303(1); *Digital Signature Guidelines* § 4.3.