# WHAT SECURE ELECTRONIC SIGNATURE TECHNOLOGIES ARE PERMITTED UNDER THE E-SIGN ACT AND UETA, AND DOES EACH METHOD PROVIDE ADEQUATE PROTECTION AGAINST ELECTRONIC FRAUD?

By Allison K. Fong

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Information Science.

Chapel Hill, North Carolina

April, 2001

Approved by:

______________________________

Advisor

Allison K. Fong. What Secure Electronic Signature Technologies Are Permitted Under the E-Sign Act and UETA, and Does Each Method Provide Adequate Protection Against Electronic Fraud? A Master's paper for the M.S. in I.S. degree. April, 2001. 38 pages. Advisor: Gregory B. Newby.

This paper discusses the technology-neutral statutes that enable electronic signatures and records to be accepted in lieu of manually signed paper records. In part II, the paper focuses on the language provided by the federal Electronic Signatures in National and Global E-Commerce Act ("E-Sign Act") and the model Uniform Electronic Transactions Act ("UETA"), which states may adopt. The various electronic and digital technologies and how they work are discussed in parts III and IV. Part V describes the various positive and negative security considerations. Recommendations as to the appropriate level of security necessary for electronic transactions are offered in part VI.

Headings:

Digital Signatures

Electronic Commerce

Electronic Signatures

Identity Theft—Electronic Transactions

Online Security

Public Key Infrastructure (PKI)

## Table of Contents

## I. Introduction

Traditional business transactions were conducted in person. Contracts and other documents were signed by hand, and these signatures indicated proof of identity and intent to be bound by the contract. The signing of a contract often was witnessed, acknowledged, or notarized to further assure the identities and intent of the parties. However, computer-generated documents with a name typed as the signature do not provide any assurances. In e-mail, it is possible for a person to type someone else's name as the "signature" and also mask the sender's identity and address or send it anonymously. The recipient might think the message came legitimately from the person indicated and act on the message. For important, private, or sensitive information, an unsecured transaction that can be observed or altered by others is not desirable.

Electronic commerce (e-commerce) has become big business. With the proliferation of business transacted on the Internet, the need for security has also increased.[1] People and companies want assurances that their electronic transactions are secure. The authentication provided by digital signatures is critical, since people often falsify their identities or personal information online. In a study conducted by the Graphic, Visualization & Usability Center at the Georgia Institute of Technology, "48.6% of more than 10,000 respondents indicated that they never provide false information. This means that more than half of the respondents do actually report false information." Therefore, based on estimates of the online consumer population, "more than 18 million

American consumers [falsified] their identities or personal information online by late 1999."[2]

First, this paper will discuss the requirements of the Electronic Signatures in National and Global E-Commerce Act[3] ("E-Sign Act") and Uniform Electronic Transactions Act[4] ("UETA") for electronic signatures, followed by a discussion of the current electronic signature technologies available. After reviewing the electronic technologies available, an overview of the problem of identity theft will highlight the security concerns of e-commerce consumers and providers. In the final section, this paper will recommend which electronic signature technologies are appropriate for use and the level of security they provide.

## II. The E-Sign Act and UETA: What Are These Laws?

### A. E-Sign Act

In essence, the E-Sign Act prevents states from denying legal effect to electronic documents solely due to their electronic form, thereby raising barriers to e-commerce. It promotes electronic commerce by establishing that electronic technology satisfies the traditional writing requirements for paper documents, an intent expressed by legislators in their Congressional Record Statements.[5] The statute is technology-neutral in that it does not give greater or lesser status or effect to specific technologies or specifications. In relevant part, the E-Sign Act states:

> § 101.—General Rule of Validity
> (a) In General.—Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce—
> (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
> (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.[6]

As used in this statute, "electronic" relates to "technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities."[7] An "electronic signature" is defined broadly 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."[8]

Pursuant to the E-Sign Act, § 102(a), states may modify, limit, or supersede the provisions of § 101 with respect to state law only if such statute adopts the UETA as approved and recommended by the National Conference of Commissioners on Uniform

State Laws (NCCUSL) in 1999 or provides for alternative procedures or requirements for the use and/or access of electronic records or signatures for legal effect consistent with the E-Sign Act. These alternative laws must be technology neutral in order to satisfy the E-Sign Act's requirements.[9]

### B. UETA

UETA supports use of electronic commerce by establishing legal recognition of electronic records, signatures, and contracts, and by providing procedural rules for conducting electronic transactions. Like the E-Sign Act, it states that a record or signature cannot be denied legal effect or enforceability solely due to its electronic form and an electronic record satisfies the legal writing requirement for records and signatures. In relevant part, UETA states:

> (a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
> (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
> (c) If a law requires a record to be in writing, an electronic record satisfies the law.
> (d) If a law requires a signature, an electronic signature satisfies the law.[10]

Like the E-Sign Act, UETA defines "electronic" as "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities"[11] and "electronic signature" 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."[12]

While both the E-Sign Act and UETA contain similar language that electronic signatures shall not be denied legal effect or enforceability merely because of their form, they are not identical in coverage. UETA is more comprehensive and addresses security areas such as attribution, or "Whose signature is this?" Under UETA § 9, a person cannot be bound to a record if that person's name was not entered, ratified, or provided by someone acting on behalf of that person. An electronic record or signature can be attributed to someone only if it was a act of that person, which can be established by relevant evidence, including technological or password information that can establish identity.[13]

## C. What Law Controls?

### 1. E-Sign Act's Scope

For states that do not enact UETA or other electronic records and signatures legislation, the E-Sign Act governs electronic transactions and records. Where a state has enacted UETA or other technology-neutral legislation, those laws control intrastate transactions and the E-Sign Act governs interstate and foreign transactions.[14] The E-Sign Act also promotes use and acceptance of electronic signatures internationally.[15] Where a state has enacted a modified UETA or other electronic validation laws, those laws must be reviewed under E-Sign Act § 102(a)(2). According to Nimmer, federal policy indicates "a narrow deference to state sovereignty on matters involving electronic records and signatures."[16] The E-Sign Act was not intended to preempt state law because 1) it does not expressly state that intent and 2) states are allowed to make choices without restricting the technology-neutral requirement. Since the E-Sign Act does not occupy the whole field, state laws that do not conflict with it are permitted.[17]

### 2. Technology-Specific Statutes

Several states have adopted UETA or other electronic records and signatures legislation. There are three main groups of statutes, ranging from minor to major changes of the E-Sign Act and UETA language.[18]

Utah enacted the first digital signature legislation in 1995,[19] based on the Digital Signature Guidelines promulgated by the American Bar Association Security Committee.[20] This statute provides that records utilizing dual public key encryption with third-party certification will be attributed to, and be legally binding on, the person who has been issued that key. While the Utah statute does not invalidate any other signature technologies that may be valid, it has accorded greater legal status or effect to records or signatures utilizing public key encryption.[21]

Illinois has enacted a statute containing general language approving electronic signatures, but provides that "secure" signatures and records will receive heightened legal effect.[22] A "secure" electronic signature or record is created by agreement of the parties or upon certification by the Illinois Secretary of State.[23]

California provides that an electronic signature has the same force as a manual signature if: 1) it is unique to the person using it; 2) it can be verified; 3) the person using it maintains sole control over it; and 4) it conforms to regulations adopted by the Secretary of State. [24] The Secretary of State has promulgated regulations that are technology-neutral and that do not regulate the licensing or approval of Certification Authorities. Digital signature technology and signature dynamics are both acceptable if they provide signatures in conformity with the statute.[25]

### 3. Does the E-Sign Act Preempt Nonconforming State Laws?

State law that does not conform to the requirements of E-Sign Act § 101 will be evaluated under § 102(a)(2). Since the legislative history comments state that laws with any variation from the exact UETA document may or may not be eligible under § 102(a)(2), Nimmer interprets it as placing the entire statute at issue under § 102(a)(2) and not just the nonconforming provisions because it is not an adoption of the UETA exactly as approved by NCCUSL.[26] However, others argue that only nonconforming provisions of an enactment should be evaluated under § 102(a)(2), thus rendering only the inconsistent provisions ineffective while saving the remainder of the statute.[27] Fry considers two other possible readings of the preemption language but finds both to be less persuasive:

> Under one, if the State statute has any non-uniform provision, the entire enactment is ineffective and federal law governs. Such as reading would be consistent with the literal language of subsection (a)(1) and would force the entire packet of State legislation to be evaluated for consistency and in terms of medium neutrality under subsection (a)(2). Under the second, but least persuasive alternative reading, non-uniform provisions do not survive, whether or not they would be acceptable under subsection (a)(2).[28]

Whether preemption requires an entire nonconforming statute or just the nonconforming portions of a statute to be reviewed and possibly preempted has not been decided through case law. As the law develops in this area, court decisions or legislation will clarify the issue.

## III. Electronic Signatures

### A. Signatures

What is a signature? It is any mark made with the intention of authenticating the marked document.[29] The law defines a signature as a symbol, even an X, a thumbprint, or sometimes a corporate letterhead, adopted with the intent to comply.[30] Marks fulfilling this definition have been used throughout history. To make a contract under Roman law, a citizen pressed his signet ring into a wax tablet. During the Middle Ages, Europeans affixed a clay seal to a document to authenticate the marked contract. Later, parties to a contract hand-scripted their signatures.[31] Webster's Dictionary defines a signature as "the name of a person written with his or her own hand."[32]

What is an "electronic signature"? Under the Webster's Dictionary definition, an electronic signature is not a signature at all. An electronic signature is "any symbol, mark or method, accomplished by electronic means, executed by a party with the present intent to be bound by a record or to authenticate a record."[33] An electronic signature can be any electronic mark signifying agreement. This definition covers a wide range of signature types—from digitized images of a handwritten signature to a retinal scan. Some electronic signatures are very secure. A retinal scan, for example, is almost impossible to duplicate. Other electronic signatures are less secure, such as a handwritten signature that can be scanned, saved as a computerized image, and used to "sign" documents.[34]

A signature implies uniqueness and is associated with a person's identity. The tiny differences that are "a reflection of physical and psychological identity" mean that no two signatures are identical, but they also dictate that two signatures by the same person will be much more alike than the same signature produced by two different people.[35] Thus, “geometric uniqueness” establishes authenticity for handwritten signatures.[36] However, in the digital world, the computer can copy or alter geometric representations, so another method is needed to establish signature uniqueness or signature authenticity.[37]

### B. Biometrics

Biometric methods offer another form of secure electronic signatures that promise a high level of security. Unlike digital signatures, which rely on authentication, biometric security relies on proof of identification. It involves measuring and recognizing some unique biological aspect of, or physical act performed by, a particular human being. Examples of biometric technologies include fingerprint imaging, voice recognition, retina scanning, and facial recognition.[38]

These biometric techniques can be practical and reasonably priced. Biometrics also offers the advantage of quick and secure verification of a person’s identity in routine transactions. Finger imaging, voice recognition, and the stylus and digitizer technologies can be installed on a personal computer. Retina scanning or finger imaging could replace the use of personal identification numbers (PINs) at ATM machines, while smart cards containing biometric information could be used in place of credit cards, debit cards or driver’s licenses.[39]

In addition, other forms of biometric authentication may be incorporated into digital authentication protocols. For example, a biometric fingerprint or eye scan authentication system might be used in a hybrid system instead of a passphrase to protect the private key in a cryptographic system. Many of these methods have different levels of reliability and utility for digital authentication. Companies involved in biometric identification admit that while units are sophisticated in detecting fraudulent identifiers, such as recordings of voices or copies of fingerprints, the output data of the biometric reader is susceptible to interception as it is transmitted for verification. These security technologies serve as a warning that states should expect the development of other secure technologies and not that other technologies are ready for "prime time" at present.[40]

### C. Signature Representations

Other technologies may be able to create electronic signatures of approximately equal security to cryptographic signatures, such as signature dynamics technology. Signature dynamics systems digitally record a manual signature with a special stylus and digitizer pad.[41] The digitizer pad analyzes many biometric measures of signature behavior such as the time taken to complete a signature, including pauses between strokes, points, curves, the pressure applied on the pen pad at various points in the signing process; the overall size of the signature; the form and shape of the signature; the length and angle of lines, arcs, and curves; the number of loops, slopes, velocity, and acceleration; and other features of a handwritten signature, creating a "biometric token."[42] This biometric token can be transmitted to authenticate a digital document[43] and provide evidentiary information for comparison against future signatures. This method provides security against fraud and forgery while "retaining the ceremonial aspects of a traditional signing."[44]

Electronic signatures are different from digital signatures, which are discussed in part IV. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad connected to the system.[45] Signature dynamics is a biometric input capturing method because it measures human-dependent characteristics. Human signatures are reflexive actions not subject to deliberate muscular control, so imitation of a signature is difficult. Since a person cannot manually produce two identical handwritten signatures, computerized comparisons cannot be based on a bit-to-bit comparison, but through statistical and probability tests. Most dynamic electronic signature verification systems today are approximately 96 percent accurate when the signer is relatively consistent. Accuracy decreases with inconsistent signers or when wear and tear affects the equipment.[46]

## IV. Digital Signatures

### A. What Are They?

Although the terms “electronic signature” and “digital signature” are often used interchangeably, “digital signature” is a special type of electronic signature.[47] “Electronic signatures” is a broader term that applies to any signature in electronic form, including a name typed at the end of an e-mail message.[48] “Digital signature” is a term of art for computer encryption technology that provides secure signatures on electronic documents, such as public key infrastructure.[49] Digital signatures authenticate electronic documents in much the same way that handwritten signatures authenticate printed documents.[50]

A digital signature is not the same as an electronically stored handwritten signature. The phrase “digital signature” has been called “the most unfortunate nomenclature mistake in the history of cryptography”[51] because it is not like a traditional manual signature. A digital signature is a computer-entrusted code that protects the authenticity of electronically filed documents, guarding against tampering and assuring both parties that the transmitted information is complete and accurate.[52] It is a string of bits that uniquely represents a second string of bits, the digital document. It is formed using a combination of software techniques and cryptography, based on a secret value known only to the signer. Unlike a human signature, a digital signature is unique to each document signed digitally, although the secret value remains the same. To verify that a digital signature is valid in public key encryption infrastructure (“PKI”), there is a corresponding verification function and a public key that uniquely identifies or represents the signer.[53]

## B. How Does It Work?

### 1. In General

There are two kinds of digital signatures: "signatures good enough for a six dollar trade among friends, and signatures good enough for a six figure trade between strangers."[54] The first type is called symmetric, or single key, encryption. The same key is used to encrypt and decrypt the document. For example, Alice and Bob agree on an algorithm and a key. Alice encrypts a message with the key and sends the ciphertext to Bob, who then decrypts it with the same key.[55] The message is secure only if third parties do not know the key.[56] Single key encryption is analogous to a combination safe, where people placing items into and taking them out of the safe must be able to open the combination lock.[57]

The second type of digital signature is public key, or asymmetric, encryption,[58] often referred to as public key infrastructure ("PKI").[59] In a public key system, Bob generates two different but corresponding keys. The public key can encrypt messages and the private key can decrypt the first key's resulting ciphertext. Bob can now publish the public key for Alice to encrypt her message to him, secure in the knowledge that Eve (who lacks the private key) cannot decrypt the message. "Public key encryption is analogous to a post office box, where anyone can deposit mail once the recipient's specific box number (the public key) is known, although only the box holder with the (private) key can open the box."[60] This system is better suited for communication over open networks such as the Internet, because there is no secret key that must be protected.[61] Under this system, communications to groups require more steps. The message must be encrypted for each recipient's private key, like placing a separate copy of the message, uniquely coded, in Bob's, Carol's, and Dave's post office boxes. Also, using a public key algorithm is "roughly a thousand times [slower than using] a symmetric algorithm."[62]

In practice, PKI programs are actually hybrid systems. In these systems, the public keys are used only to encrypt and securely transmit a symmetric encryption key called a session key. The session key is used to encrypt and decrypt the content of a specific communication, and is not reused after that communication is completed. This system avoids the problem of needing a secure channel to communicate keys in a symmetric system, and the slowness of using public key cryptography alone.[63]

There are two public key infrastructure ("PKI") models, the "open" and "closed" models. The term PKI usually refers to the services and protocols that support the application of public key cryptography, including: obtaining or generating a party's public key; the issuance of a digital certificate for a public key by a Certification Authority (CA); cancellation of a public key if the private key is lost or compromised; and a methodology for evaluating whether a certificate is valid and its authorized operations. An open model assumes that a subscriber obtains a digital certificate from a CA that will securely link her identity to her public key for all, or at least many, purposes. Thus, in an open PKI environment, a person could obtain a digital certificate and then use it for a transaction requiring a digital signature such as ordering goods online, signing legally binding agreements, and filing documents with a government entity. In the closed PKI model, users obtain a different digital certificate for each online use. The difference is significant. In an open PKI model, a person's certificate could potentially sign any document, resulting in severe consequences if the private key is compromised. In a closed PKI, the risks of a fraudulently signed document are more limited because of the system's more narrowly defined scope.[64]

### 2. The Technical Procedure

The phrase "digital signature" is a term of art for a process whereby a mathematical formula secures and authenticates a message. A digital signature requires two processes: 1) PKI, a particular method of using mathematical algorithms to scramble a communication, and 2) a hash function to verify the integrity of a message. With a public key system, the software generates two related keys—a public key and a private key. The public key is available for anyone to know, while the only the owner knows the private key. Only the public key can decrypt a message encoded with the private key, and only the private key can decode a message encoded with the public key.[65] A hash function is a process used to verify the integrity of a message. This procedure creates a number, the message digest, which represents the message. The algorithm produces a message digest uniquely based on the data in the message that cannot be reproduced if the message has been altered. Any change to the message produces a different message digest.

The technology works as follows. After writing his message, the sender performs the "hash function" to generate the message digest, a string of code. The sender then encrypts this message digest with his private key, attaches this "signature" to the end of the document, and sends the "signed" document to the recipient. The recipient, using the same software, can perform a hash function on the message. If the message digests are identical, the recipient knows that the message was not altered during transmission.[66]

### 3. Certificates of Ownership

#### a. Additional Assurance

Another important element in the chain of document security is the certificate, a digital document attesting that a particular public key has been given to an individual or entity.  It verifies that a given public key does in fact belong to a given individual, much like presenting photographic identification at the bank.[67]

This association of a digital signature with an individual's identity must also be verified. Currently, anyone can create a public key-private key pair in the name of any particular person and upload it to databases of public keys.[68]  How does one confirm that the individual who created the key for "Elmer Fudd" *is* Elmer Fudd? Without independent verification, the public key of Elmer Fudd may be a fraud perpetrated by an imposter purporting to be the true Elmer Fudd.  People may unwittingly rely on a fraudulent digital signature. Therefore, digitally signed messages purporting to be associated with an individual identity should be attested to by a trusted third party, a certification authority, to minimize the occurrences of fraudulent representations.[69]

Certification authorities ("CAs") maintain repositories of public keys and authenticate and legitimize the relationship between a person and a particular public key.[70]  A repository is "an electronic database of certificates—the equivalent of [an online] digital Yellow Pages" accessible to the general public.  Unlike the Yellow Pages, however, a user may be charged for access to the information.[71]

### i. Obtaining a Certificate

First, the subscriber generates a public key-private key pair. He then visits the CA in person with proof of his identity. A driver's license and/or passport is acceptable, since either is an official document with a photograph. The subscriber then demonstrates that he has the corresponding private key to a public key-private key pair without disclosing it, usually by sending a digitally signed electronic message in the presence of the CA.[72]

Once the CA verifies the association between an identified person and public key, it issues a certificate, an electronically stored record attesting to the connection between the public key and the subscriber. The certificate identifies the issuing CA, the subscriber, and the subscriber's public key. It may also contain other relevant information, such as the key expiration date, size, and a signature generation software identifier.[73] A CA may give notice of the creation and contents of a certificate by providing the subscriber with a printed representation of the certificate; by allowing the subscriber to view the contents of the certificate online; or by communicating the content of the certificate to the subscriber in any other reasonable way, such as by first-class mail. The CA attaches its own digital signature to the certificate if it is sent electronically.

Once the CA issues a certificate, the subscriber must review its contents to ensure accuracy before the certificate is made publicly available. The subscriber must accept the certificate for both verification and validation. After the subscriber has reviewed the contents of the certificate and is satisfied with the certificate's accuracy, he or she may publish the certificate or direct the CA to do so. Once the CA publishes the certificate, it represents that the subscriber has accepted the certificate, and the certificate is given a presumption of validity.[74]

### ii. Using the Certificate

When a certificate is published, it is made available to third parties. A certificate is published when it is recorded in a repository, or otherwise circulated, and made accessible to all parties desiring to correspond with the subscriber. When the subscriber wishes to send a message, he or she would send the message along with a message digest and a certificate that links him to the public key. The recipient can then go to an online database to check the validity of the certificate.[75]

The most secure use of authentication involves enclosing one or more certificates with every signed message. The recipient verifies the certificate using the certifying authority's public key. He or she then verifies the message's signature. Two or more certificates could be enclosed with the message, forming a hierarchical chain wherein one certificate testifies to the authenticity of the previous certificate, similar to current methods of establishing personal identity with multiple official identification documents.[76] The CA's digital signature can be verified by using the public key of that CA listed in another certificate issued by another CA, and that certificate can then be authenticated by the public key listed in yet another certificate, and so on until a satisfactory level of trust regarding the original certificate is achieved. The digital certificate can also contain additional information, including a reliance limit or a reference to the CA’s “certification practice statement” that gives relying parties notice of the level of inquiry conducted by the CA before issuing the certificate.[77]

### b. Compromised Certificates

A private key, like a physical key, must be physically safeguarded. If a third party discovers the private key, the security of all communications using that private key is compromised. When the private key is either lost or compromised, the individual should immediately suspend or revoke the corresponding certificate. The certificates stored at a repository usually contain the status of the certificate, such as whether the certificate is “valid,” “suspended,” or “revoked.” Revoked certificates are also stored on a Certificate Revocation List (“CRL”), which is a separate database of certificates and their corresponding public keys that have been revoked before their expiration date.[78]

## V. Security Issues

### A. The Threat of Identity Theft

Identity theft is the illicit use of a person's personal information or identifying facts, such as name, date of birth, Social Security Number, address, or other information, to perpetrate fraud. In the past, identity information was commonly stolen through pickpocketing, taking pre-approved credit applications from mailboxes, or finding receipts in the trash. Today, thieves can use credit reports to acquire false identity cards, open credit accounts, and run up large debts against innocent victims.[79] In extreme cases of identity theft,

> a perpetrator may wholly co-opt another person's identity—obtaining driver's and professional licenses, obtaining employment, applying for apartments, taking out home and automobile loans, applying for credit cards, and even receiving traffic tickets and warrants under the false identity.[80]

Eventually the imposter may file bankruptcy proceedings to discharge the debt, which is when some victims first learn of the crime.[81] Identity theft is now a federal offense.[82]

Businesses want "the ability to predict, with a fair degree of certainty, what lies ahead in our daily lives, the ability to control it, and the ability to identify, again with a fair degree of certainty, the risks that we may face so that we can take protective measures."[83] Businesses involved in e-commerce want to secure online transactions, which require entering into agreements that both parties believe will be performed. On the Internet, the person with whom you are dealing may not be who he or she claims to be, as is demonstrated by the proverbial cartoon: "On the Internet, nobody knows you're a dog."[84] Electronic transactions must be secure so that parties have reasonable assurance that they are dealing with people who actually are who they say they are. Both businesses and individuals are investing in encryption technologies to protect their proprietary information and communications, protect their privacy, and prevent theft, industrial espionage, and identity theft.[85]

How can someone ascertain that a person is who he claims to be, especially at the initial Internet contact? A first-time contract should be protected by strong security measures. One relatively secure method is

> by sending paper copies through the postal service to a bricks-and-mortar address supplied by the customer, which copies are hand signed and returned by the customer as proof of attribution. In this case, identity may be inferred from a number of indicia, including the presence of a person at a physical address to receive a postal letter, and calligraphic signature evidence. In the online analog, the identities associated with electronic signatures on first-time contracts must also be inferred by indicia that are at least as reliable as those for paper contracts. One technology with promise for bridging the gap at time of enrollment involves the use of "digital signatures" as an electronic means to associate a real identity with an electronic signature.[86]

## B. What Is Needed?

With the pervasive use of computers today, many organizations and institutions would like to conduct more of their activities through electronic means. However, the increased use of computer technology has not eliminated the need to ensure the completeness, accuracy and authenticity of legally signed electronic documents. It is now necessary to find digital equivalents that ensure authenticity, integrity, and non-repudiation. Authentication ascertains the originator of a digital document, to protect against imposters. Integrity is necessary to verify that a digital document has not been altered in transit or replaced by a false document. Finally, non-repudiation ensures that the sender cannot later deny that he sent the document.[87] Laws that validate e-commerce provide legal security for enforcing electronic transactions and setting forth the rules for such transactions. Without a clear legal framework, encryption or authentication technology will not provide adequate security for electronic business transactions.[88]

### C. Advantages of Using Digital Signatures

Traditional handwritten signatures are vulnerable for several reasons. First, there is no standard for a handwritten signature, so they can vary, making signature verification difficult. Second, handwritten signatures can be easily forged or copied. Finally, on multiple page documents, it may be unclear whether the signature applies to all pages or whether pages have been added or deleted since the signing. By comparison, digital signatures have features that provide a higher level of security over handwritten signatures.[89]

First, a key feature of digital signatures is proof of data integrity, or the assurance that the data has not been accidentally or intentionally altered. The message digest or hash algorithm fulfills this function since it is unique to the document. It indicates if any unauthorized or accidental changes have occurred.[90]

Second, authentication answers the question, “Who sent this message?” The answer to this question has been important even for handwritten signatures, which are not considered legally binding in and of themselves. Any signature, handwritten or electronic, must be authenticated. This was traditionally done through a notary public. In the digital world, CAs provide the necessary authentication, and the certification becomes inextricably part of the document.[91]

Third, non-repudiation is particularly important in electronic commerce. The signer and recipient of a document cannot deny the existence or integrity of the transaction secured by digital signature technology. Three things provide proof of the transaction and ensure its integrity: 1) the existence of the original message; 2) the associated encrypted message digest; and 3) the attached digital certificate. If the transaction was questioned, it could be proven that “the sender’s public key decrypts a given message digest; the message digest corresponds to the message in question; and the relevant certification authority listed the sender’s certificate as valid at the time of the transaction.”[92]

Fourth, most digital signature technologies include a date and time stamp function that can be critical for use in electronic commerce and legal actions. This is critical to the implementation of digital certificates because the date and time will be used to verify whether the digital signature was created during the operational period stated in the certificate.[93]

Fifth, according to IBM, digital signatures can increase the speed and accuracy of transactions. Documents can be signed and transmitted around the world in just a few seconds. Digital documents and signatures can be processed faster and more accurately by automated systems than a human being can evaluate a handwritten signature. Thus, the speed and security of digital transactions is enhanced through the use of digital signatures.[94]

Finally, digital signature technology can increase confidentiality, ensuring that only the appropriate recipients can decrypt the message because only they have access to the appropriate key. Although there is no control over what happens to the message after it has been decrypted, unauthorized access is protected during transmission, which is the most critical and vulnerable period.[95]

## D. Concerns About Digital Signatures

### 1. What Do Digital Signatures Secure?

Digital signatures prove, mathematically, that a secret value known as the private key was present in a computer at the time the subscriber's or sender's signature was calculated. It is a small step from that to assume that the sender associated with the private key entered that key into the computer at the time of signing. But it is a much larger step to assume that the sender intended a particular document to be signed. And without a tamperproof computer trusted by the sender, digital signatures can be contested.[96]

While a digital signature authenticates the document up to the point of the signing computer, it does not authenticate the link between that computer and the person composing the document. The computer signs the document, not the person.[97] In some instances, authenticating to the signing computer is good enough, and no further authentication is required. However, for sensitive materials, this complaint should be considered:

> [C]ryptography, no matter how strong, cannot bridge the gap between me and my computer. Because the computer is not trusted, I cannot rely on it to show me what it is doing or do what I tell it to. Checking the calculation afterwards does not help; the untrusted computer can't be relied upon to check the calculations properly. It wouldn't help to verify the code, because the untrusted computer is running the code (and probably doing the verification). It wouldn't even help to store the digital signature key in a secure module: the module still has to rely on the untrusted computer for input and output.[98]

### 2. Security Loopholes

One of the most obvious and most common security problems with digital signatures is the human error factor. There are several points at which human error can create problems. If a private key is lost, stolen, or shared with someone other than its owner, then that private key is no longer a reliable factor in the creation of digital signatures.[99] Human error can also be a problem for digital certificates. Inevitably, someone will type in a name or word incorrectly, resulting in an inaccurate certificate.[100] Unintentional errors by owners of private keys include lost or publicly displayed passwords, password sharing, and terminals left unattended after logging on. Intentional human breaches of security include theft of passwords or private keys, tampering with the technological systems, or altering or forging the text of digital documents.[101]

Many users are also concerned about the extreme sensitivity of private keys. Lost keys are impossible to regain, and a user who loses a key and is assigned a new one will have difficulty reestablishing his or her identity. This issue, which has no widely accepted solution, must be addressed by any organization using a digital signature system.[102]

Additionally, digital signature passwords, private keys, and certificates must necessarily be stored somewhere, whether on paper or in electronic form. There is the potential of losing electronic data. The CA's repository may be lost and unrecoverable due to technical failures. Another access issue is whether unauthorized or illegal access to key and password data is possible. In some situations, anyone with access to the software program can compromise others' private keys. Criminals in possession of the appropriate data could masquerade as someone else and perform electronic transactions using that person's authorized key.[103] It may be possible to store and backup a private key with multiple individuals or organizations so that cooperation between many people is necessary to access the key. This may provide sufficient security for secondary backup.[104]

Reliance on CAs can also create security issues. The digital certificate provided by a CA is a digital signature message from the issuer (signer or CA) to the verifier (user) that associates a name with a public key. There are five issues to consider: 1) The signer may be compromised through theft. CA's protect against this possibility with either strong network, physical, and personnel security or independent signatures on the same certificate. 2) How did the signer know the information being certified? A good signer should personally know the person and have proof of identity before certifying someone's identity. Some CAs, however, rely on public database information that is for sale, such as credit bureau information. 3) Did the issuer verify that the keyholder controlled the associated private key? This proof would strengthen the presumption that the person's identity was correct. 4) Did the user or receiver check to see if the key or certificate was revoked or suspended? 5) How are the computers of the sender and receiver protected? Are terminals accessible to others? Can the codes be tampered with or accessed easily? Can someone send a message from one terminal with that person's electronic identity attached to the message?[105]

PKI and digital signature technologies are almost completely secure against hacking and cracking. While it is mathematically possible to break the algorithmic code, the time and resources needed to do so make it unlikely. However, someone will eventually develop a new technology that will make it feasible. The likelihood of this occurrence may depend on the strength of the algorithm used. [106]

### 3. Costs

As with almost all forms of technology, digital signature capabilities are not free. The institutional cost to the public may be significant, depending on the ability of decision-makers to plan effectively. Creating or designating CAs or trusted third parties may be costly. At a minimum, existing institutions will need to spend money training their representatives to explain and sell the keys and software. At the opposite extreme, it will be expensive to create new institutions, establish accreditation procedures, and determine how to license and audit CAs. There are also individual costs that a single user or a corporation must incur to purchase the actual software and keys from a CA. The calculation of whether these costs exceed the benefits of creating a more predictable commercial and legal environment depends on whether policymakers can appropriately design and enact legislation that addresses the benefits and costs of digital signatures.[107]

## E. Enhancing Security

### 1. Total Document Encryption

Instead of encrypting just the message digest, or digital signature, encryption systems based on the federal Digital Encryption Standard (DES), or alternatives such as the Rivest-Shamir-Adleman (RSA) algorithm[108] can be used to encrypt entire documents.[109] Although encrypted digital signatures are more efficient than encrypted documents, sensitive materials may warrant encryption of the entire document.

### 2. Digital Notarization

Digital notarization, a digital time stamp that indicates when a document was created, transmitted, received or processed, can provide protection for the integrity of a digital document’s contents as well. A Digital Notary System based on patented time-stamping protocols is commercially available today.[110]

### 3. A Combined Electronic and Digital Signature Technology

"The tendency of using a hammer to solve all our knocking problems is always there."[111] Some biometrics product vendors claim that dynamic electronic signatures are more secure than the digital signature technologies discussed above.

In the dynamic electronic signature method, the digital document signature also is hashed into a message digest. However, the dynamically captured electronic signature is appended to the document. The message digest and the electronic signature are then bound together by applying encryption of the concatenation with a secret key. To implement this method, there must be a process to capture a valid version of the person's biometric characteristics in the system. The registration process is necessary to ensure that the digital certificate required for verification purposes is issued to the correct person requesting it. By combining an electronic signature and digital signature scheme, the registration process can be combined to "deter any would-be perpetrator from impersonating another person since such biometrics data provide [sic] an audit trail for the impersonator to be identified positively in the near future."[112] "There always needs to be an auditable event, something that lets people know why this person is signing."[113] If this combined technology results in greater certainty for people's identities, and it is not cumbersome or costly to implement, Kang's suggestion may be the next level of secure digital signatures.

## VI. Recommendations

For the cautious, a higher level of security is preferable if it is not prohibitively time-consuming or expensive. While there are many electronic technologies that meet the technology-neutral language of the E-Sign Act and UETA, at least one author believes that digital signature encryption (PKI) will be the *de facto* standard of e-commerce transactions:

> Although hindsight after actual experience will obviously be the best teacher, the authors believe that PKI digital signatures will ultimately be recognized as providing a robust factual inference of identity—perhaps to the point that technologic neutrality and pre-emption of any legal presumption or other favorable legal status for PKI digital signatures will essentially not make much difference. This inference will at first need to be established in the early litigated cases by appropriate expert and factual testimony showing that the digital signature process produces an accurate result. But over time it can be expected that the need for this foundation will ultimately diminish or wither away as courts become more familiar with PKI digital signatures.[114]

If PKI becomes the standard, businesses and individuals who require even more protection are likely to adopt total document encryption technologies, such as RSA or a combination of electronic and digital signature technology as suggested by Kang. With all of the security issues that must be addressed, prudent businesses and individuals should balance their need for security against their need for efficiency or speed and utilize the technology or combination of technologies that provides them with the best protection without seriously affecting whatever other considerations are important to them.

## VII. Conclusion

The mainstreaming of Internet transactions has increased the need for secure electronic documents.  Electronic technologies have been created to meet the needs for authenticity, confidentiality, and security.  While electronic signatures using biometrics methods or representations of handwritten signatures are available, digital signatures, an encryption technology, offers the most security.  Digital signatures encryption technology comes in many forms and can be implemented with varying levels of security.  This paper has provided an overview of the technologies available and considerations to take into account when choosing the level of assurance needed for a transaction.

**Notes**

[1] Dan Briody, *Digital Signatures Create Market Potential: How Will Companies Make Consumers Feel Secure Enough to Sign on the Digital Line?* 22 InfoWorld 35 (Jul. 24, 2000).
[2] Kalama M. Lui-Kwan, *Article: VI. Business Law*, 14 Berkeley Tech. L.J. 463, 465 (1999).
[3] Pub. L. 106-229, 114 Stat. 464 (2000).
[4] Uniform Electronic Transactions Act, National Conference of Commissioners on Uniform State Laws, Draft (1999).
[5] Raymond T. Nimmer, Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws (2000) (unpublished manuscript) (last visited Apr. 16, 2001) <http://www.bmck.com/ecommerce/topic-esignatures.htm>.
On pages 1-2, Nimmer notes that:

> For example, one sponsor commented:
>
> [This Federal Act] is founded on a simple premise. Any requirement in law that a contract be signed or that a document be in writing can be met by an electronically signed contract or an electronic document. We are simply giving the electronic medium the same legal effect and enforceability as the medium of paper.
>
> The statement of another leading legislative figure in enactment likewise carves out a narrow but important, focused goal for the Federal Act:
>
> [The Federal Act] will eliminate the single most significant vulnerability of electronic commerce, which is the fear that everything it revolves around—electronic signatures, contracts, and other records—could be rendered invalid solely by virtue of their being in “electronic” form, rather than a tangible, ink and paper format. This [Act] will literally supply the pavement for the e-commerce lane of the information superhighway.

[6] 106 P. L. 229, 114 Stat. 464 (2000).
[7] *Id*. at § 106(2).
[8] *Id*. at § 106(5).
[9] *Id*. at 102(a), which states:

> § 102.—Exemption to Preemption.
>
> (a) In General.—A State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of section 101 with respect to State law only if such statute, regulation, or rule of law--
>
> (1) constitutes an enactment of adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999, except that any exception to the scope of such Act enacted by a State under section 3(b()4) of such Act shall be preempted to the extent such exception is inconsistent with this title or title II, or would not be permitted under paragraph (2)(A)(ii) of this subsection; or
>
> (2) (A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if—
>
> (i) such alternative procedures or requirements are consistent with this title and title II; and
>
> (ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures;

[10] UETA, § 7 (1999).
[11] *Id*. at § 2(5).
[12] *Id*. at § 2(7).
[13] Patricia Brumfield Fry, *A Preliminary Analysis of Federal and State Electronic Commerce Laws*, § 2(a) (2000) (last visited Apr. 16, 2001) <http://www.bmck.com/ecommerce/topic-esignatures.htm>.

[14] Charles R. Merrill & Robert J. Burger, *E-Quality at Last for E-Signatures: Statutory Changes Afoot May Finally Release E-Commerce from the Bonds of Ink and Paper*, N.J.L.J., Aug. 21, 2000 (last visited Apr. 16, 2001), at ¶ 8 <http://www5.law.com/nj-shl/display.cfm?id=3226>.

[15] 106 P.L. 229, 114 Stat. 464 § 301(a)(1) (2000) states in relevant portion:

> § 301.—Principles Governing the Use of Electronic Signatures in International Transactions
> (a) Promotion of Electronic Signatures.—
>
> > (1) Required actions.—The Secretary of Commerce shall promote the acceptance and use, on an international basis, of electronic signatures in accordance with the principles specified in paragraph (2) and in a manner consistent with section 101of this Act. The Secretary of Commerce shall take all actions necessary in a manner consistent with such principles to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce.

[16] Nimmer, *supra* note 5, at 8.

[17] *Id*. at 4-5.

[18] For a comprehensive list of states that have enacted or are considering enacting UETA or other electronic signature statutes, some law firms have useful websites. Baker & McKenzie, *Uniform Electronic Transactions Act (UETA State-By-State Comparison Table* (last visited Apr. 9, 2001) <http://www.bmck.com/ecommerce/uetacomp.htm>. See also McBride Baker & Coles, Law Authorizing Signatures (last visited Apr. 9, 2001) <http://www.mbc.com/ecommerce/legislative_1.asp?state--all>. Note: under the “E-Commerce Spotlight,” select “Legislative Tables,” under “Select a Legislative Table choose “Laws Authorizing Signatures” and under “Select a State Table (optional)” select “All States”.

[19] Utah Code Ann. § 46-3-101 to –504 (1998).

[20] Albert Gidari & John P. Morgan, *Survey of Electronic and Digital Signature Legislative Initiatives in the United States*, Internet Law and Policy Forum 5 (last modified Sep. 12, 1997) <http://www.ilpf.org/digsig/digrep.htm>. The Digital Signature Guidelines promulgated by the ABA are available at <http://www.abanet.org/>.

[21] Fry, *supra* note 13, at § 3, ¶ 8.

[22] 5 Ill. Comp. Stat. Ann. 175/10-110 (Supp. 2000).

[23] Fry, *supra* note 13, at § 3, ¶ 9.

[24] Cal. Civ. Code § 1633.7 (Supp. 2001).

[25] Adam White Scoville, *Clear Signatures, Obscure Signs*, 17 Cardozo Arts & Ent. L.J. 345, 379 (1999).

[26] Nimmer, *supra* note 5, at 8.

[27] Fry, *supra* note 13, at § 1, ¶ 3.

[28] *Id*.

[29] W. Everett Lupton, Comment, *The Digital Signature: Your Identity by the Numbers*, 6 Rich. J. L. & Tech. 10, at ¶ 3 (1999) (last visited Apr. 16, 2001) <http://www.richmond.Edu/jolt.v6i2/note2.html>.

[30] Briody, *supra* note 1.

[31] Lupton, *supra* note 29, at ¶ 3.

[32] Briody, *supra* note 1.

[33] Christopher B. Woods, *Commercial Law: Determining Repugnancy in an Electronic Age: Excluded Transactions Under Electronic Writing And Signature Legislation*, 52 Okla. L. Rev. 411, 414 (1999).

[34] Lupton, *supra* note 29, at ¶ 5.

[35] Joel Orr, *Identity Crisis*, 68 Civil Engineering, 52 (1998).

[36] *Id*.

[37] *Id*.

[38] Woods, *supra* note 33, at 417.

[39] However, as with all security measures, these can be circumvented. In *Demolition Man*, a criminal kills the prison warden and takes his eyeball to bypass a security gate protected by a retina scan.

[40] Scoville, *supra* note 25, at 355.

[41] Woods, *supra* note 33, at 417.

[42] Meng-Chow Kang, *Dynamic Handwritten Signature Verification System: Can Electronic Signature Replace Digital Signature?* at 4 (last modified 1998) (10 pages)

<http://www.home1.pacific.net.sg/~mckang/Rnsign.html>; Scoville, *supra* note 25, at 355; Woods, *supra* note 33, at 417.
[43] Scoville, *supra* note 5, at 355.
[44] Woods, *supra* note 33, at 417.
[45] Kang, *supra* note 42, at 4.
[46] *Id*.
[47] Lupton, *supra* note 29, at ¶ 6.
[48] Danielle Borasky & Jason Link, *All About Digital Signatures:* All About Digital Signatures: What Are Digital Signatures ¶ 1 (last modified Apr. 21, 1998) <http://www.unc.edu/courses/law357c/cyberprojects/spring98/digitalsignatures/main.html>.
[49] Lupton, *supra* note 29, at ¶ 7.
[50] Lui-Kwan, *supra* note 2, at 466.
[51] Bruce Schneier, *Why Digital Signatures Are Not Signatures*, Crypto-Gram, ¶ 4 (Nov. 15, 2000) <http://www.counterpane.com/crypto-gram-0011.html#1>.
[52] Lynne Wilbanks Jeter, *What Role Will Banks Play in E-Signature Technology?* Mississippi Business Journal, vol. 22, issue 29 at 19-20 (Jul. 17, 2000).
[53] Kang, *supra* note 42, at 4.
[54] Scoville, *supra* note 25, at 346-7.
[55] Scoville, *supra* note 25, at 350-1.
[56] Martin I. Behn, *The Illinois Electronic Commerce Security Act: Too Much Too Soon or Too Little Too Late?* 24 S. Ill. U.L.J. 201, 204 (2000).
[57] Scoville, *supra* note 25, at 351.
[58] *Id*.
[59] Phil Zinkewicz, *The Push for Digital Signature Encryption: Will It Become Increasing Presence in the Insurance Industry?* 143 Rough Notes 52 (2000).
[60] Scoville *supra* note 25, at 352-3.
[61] Behn, *supra* note 56, at 205.
[62] Scoville *supra* note 25, at 352.
[63] *Id*.
[64] Behn, *supra* note 56, at 208.
[65] Behn, *supra* note 56, at 205; Lui-Kwan, *supra* note 2, at 466-67; Woods, *supra* note 33, at 416; Zinkewicz, *supra* note 59, at 53.
[66] Behn, *supra* note 56, at 205; Lui-Kwan, *supra* note 2, at 467; Woods, *supra* note 33, at 416; Zinkewicz, *supra* note 56, at 53.
[67] Behn, *supra* note 56, at 207; Orr, *supra* note 35, at 53.
[68] Behn, *supra* note 56, at 205; Lupton, *supra* note 29, at ¶ 14.
[69] Lupton, *supra* note 29, at ¶ 14.
[70] Behn, *supra* note 56, at 206-207; Lupton, *supra* note 29, at ¶ 15.
[71] Lupton, *supra* note 29, at ¶ 17.
[72] Lupton, *supra* note 29, at ¶ 15.
[73] Behn, *supra* note 56, at 207; Lupton, *supra* note 29, at ¶ 16.
[74] Lupton, *supra* note 29, at ¶ 16.
[75] Woods, *supra* note 33, at 416.
[76] Orr , *supra* note 35, at 53.
[77] Behn, *supra* note 56, at 207.
[78] Behn, *supra* note 56, at 207; Lupton, *supra* note 29, at ¶ 18.
[79] Kurt M. Saunders & Bruce Zucker, Essay, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 Cornell J.L. & Pub. Pol'y 661, 663 (1999).
[80]Jane E. Limprecht, *On Our Watch: Fresh Start or False Start? Dealing with Identity Theft in Bankruptcy Cases*, 2001 Am. Bankr. Inst. J. 7, 9 (Jan. 2001).
[81] *Id*. at 10.
[82] 18 U.S.C. § 1028, 106 Pub. L. 578 sec. 3 (2000).

[83] Amelia H. Boss, The Internet and the Law: Searching for Security in the Law of Electronic Commerce, 23 Nova L. Rev. 583, 591 (1999).
[84] Peter Steiner, *"On the Internet, no one knows you're a dog,"* The New Yorker (pub. Jul. 5, 1993) (cartoon), (last visited Apr. 16, 2001) <http://www.cartoonbank.com/> and enter search terms "dog" and "cartoon".
[85] Kurt M. Saundersby, *The Regulation of Internet Encryption Technologies: Separating the Wheat From the Chaff*, 17 J. Marshall J. Computer & Info. L. 945, 945-46 (1999).
[86] Merrill & Burger, *supra* note 14, at "Attribution" ¶ 9.
[87] Emilio Jaksetic, *How to Ensure the Integrity of Digitally Transmitted Documents*, 6 Corporate Legal Times, Aug. 1996, at 21.
[88] Boss, *supra* note 83, at 592.
[89] ABA Section of Science and Technology, Information Security Committee, *Digital Signature Guidelines Tutorial* at 3 (last visited Sep. 1, 2000) <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>. The ABA Digital Signature Guidelines are available for free download at <http://www.abanet.org/scitech/ec/isc/dsgfree.html>.
[90] *Id*. at 3-4.
[91] Borasky and Link, *supra* note 48, at Certificate Authority Liability: Trusted Third Parties.
[92] Daniel Greenwood, *Electronic Signatures and Records: Legal, Policy and Technical Considerations*, Version 1.0 (Draft Jan. 9, 1997) (last visited Apr. 16, 2001) <http://www.state.ma.us/itd/legal/e-sig.htm>.
[93] ABA Digital Signature Guidelines Tutorial, *supra* note 89, at 6.
[94] Borasky and Link, *supra* note 48, at Digital Signatures: Security Advantages of Digital Signatures: Speed and Accuracy.
[95] Borasky and Link, *supra* note 48, at Digital Signatures: Security Advantages of Digital Signatures: Confidentiality.
[96] Schneier, *supra* note 51, at ¶ 14.
[97] *Id*. at ¶ 7.
[98] *Id*. at ¶ 10.
[99] Borasky and Link, *supra* note 48, at Digital Signature Security: Security Concerns: Human Error; Lupton, *supra* note 29, at ¶ 18.
[100] *Id*.
[101] *Id*.; Jaksetic, *supra* note 87, at 21.
[102] Orr, *supra* note 35, at 54.
[103] Borasky and Link, *supra* note 48, at Digital Signature Security: Security Concerns: Storage and Backup, citing Benjamin Wright, *The Verdict on Plaintext Signatures: They're Legal* (1994) (last visited Apr. 16, 2001) <http://www.pimall.com/nais/n.cyber.sig.html>.
[104] Graham Greenleaf & Roger Clarke, *Privacy Implications of Digital Signatures*, Invited Address, IBC conference on Digital Signatures, Sydney, Australia, § 2.2 (last updated Mar. 12, 1997) <http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html>.
[105] Carl Ellison & Bruce Schneier, *Risks of PKI: Secure Email*, 43 Communications of the American Computing Machinery 160 (Jan. 2000).
[106] Oli Cooper, *An Introduction to Modern Cryptography* ¶ 2.6 (last modified Feb. 22, 2001) <http://www.cs.bris.ac.uk/~cooper/Cryptography/crypto.html>.
[107] Lui-Kwan, *supra* note 2, at 471.
[108] Saundersby, *supra* note 85, at 953-4. Confidentiality is increased by a third party's inability to distinguish the "wheat from the chaff" and not through encryption of the data:

> In 1977, Ronald Rivest, along with Adi Shamir and Leonard M. Adleman, published and later distributed their encryption algorithm known as RSA, which became the standard in public key cryptography and which is widely used for digital signatures. In March of 1998, Rivest proposed a new method for secure data transmission over the Internet that he has labeled as chaffing and winnowing.
>
> Using this method, messages are sent electronically in a combination of "good" packets (wheat) and "bad" packets (chaff). There are two steps to sending a message; authenticating and adding chaff. The recipient removes the chaff to obtain the original message. Thus, the sender first

> breaks the message into packets, and authenticates by appending to each packet a message authentication code (MAC) computed as a function of the packet contents and a secret authentication key.

[109] Jaksetic, *supra* note 87, at 21.
[110] *Id*. at 22.
[111] Kang, *supra* note 42, at 7.
[112] *Id*. at 9.
[113] Briody, *supra* note 1.
[114] Merrill & Burger, *supra* note 14, at "Digital Signatures in the Context of E-SIGN and UETA" ¶ 5.

## Bibliography

### Statutes and Model Laws

Electronic Signatures in Global and National Commerce Act ("E-Sign Act"). 106 Pub. L. 229, 114 Stat. 464 (enacted June 30, 2000).

Uniform Electronic Transactions Act ("UETA"). National Conference Of Commissioners On Uniform State Laws, 108th Annual Conference, Denver, CO (Jul. 23, 1999). (Comments dated Dec. 13, 1999.)

ABA Section of Science and Technology, Information Security Committee, *Digital Signature Guidelines Tutorial* (last visited Sep. 1, 2000) <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>. The ABA Digital Signature Guidelines are available for free download at <http://www.abanet.org/scitech/ec/isc/dsgfree.html>.

### Articles

C. Robert Beattie, *Facilitating Electronic Commerce—The Uniform Electronic Transaction Act*, 32 UCC L.J. No. 3 (Winter 2000) <http://www.oppenheimer.com/internet/ueta.shtml>.

Martin I. Behn, *The Illinois Electronic Commerce Security Act: Too Much Too Soon or Too Little Too Late?* 24 S. Ill. U.L.J. 201 (2000).

Danielle Borasky & Jason Link, *All About Digital Signatures* (last modified Apr. 21, 1998) <http://www.unc.edu/courses/law357c/cyberprojects/spring98/digitalsignatures/>.

Amelia H. Boss, *The Internet and the Law: Searching for Security in the Law of Electronic Commerce*, 23 Nova L. Rev. 583 (1999).

Dan Briody, *Digital Signatures Create Market Potential: How Will Companies Make Consumers Feel Secure Enough to Sign on the Digital Line?* 22 InfoWorld 35 (Jul. 24, 2000).

Oli Cooper, *An Introduction to Modern Cryptography,* ¶ 2.6 (last modified Feb. 22, 2001) <http://www.cs.bris.ac.uk/~cooper/Cryptography/crypto.html>.

Carl Ellison & Bruce Schneier, *Risks of PKI: Secure Email*, 43 Communications of the American Computing Machinery 160 (Jan. 2000).

Patricia Brumfield Fry, *A Preliminary Analysis of Federal and State Electronic Commerce Laws*, (2000) (last visited Apr. 16, 2001) <http://www.bmck.com/ecommerce/topic-esignatures.htm>.

Albert Gidary & John P. Morgan, *Survey of Electronic and Digital Signature Legislative Initiatives in the United States*, Internet Law and Policy Forum (last updated Sep. 12, 1997) <http://www.ilpf.org/digsig/digrep.htm>.

Graham Greenleaf & Roger Clarke, *Privacy Implications of Digital Signatures*, Invited Address, IBC conference on Digital Signatures, Sydney, Australia (last updated Mar. 12, 1997) <http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html>.

Daniel Greenwood, *Electronic Signatures and Records: Legal, Policy and Technical Considerations*, Version 1.0 (Draft Jan. 9, 1997) (last visited Apr. 16, 2001) <http://www.state.ma.us/itd/legal/e-sig.htm>.

Emilio Jaksetic, *How to Ensure the Integrity of Digitally Transmitted Documents*, 6 Corporate Legal Times, Aug. 1996, at 21-22.

Lynne Wilbanks Jeter, *What Role Will Banks Play in E-Signature Technology?* 22 Mississippi Business Journal, Jul. 17, 2000, at 19-20.

John S. Jung, *Annual Survey of Virginia Law: Technology Law*, 34 U. Rich. L. Rev. 1051 (Nov. 2000).

Meng-Chow Kang, *Dynamic Handwritten Signature Verification System: Can Electronic Signature Replace Digital Signature?* (last modified 1998) (10 pages). <http://.home1.pacific.net.sg/~mckang/Rnsign.html> (if unable to access via this URL, type “kang” “digital signature” in a Google search and click on the appropriate link.

Jane E. Limprecht, *On Our Watch: Fresh Start or False Start? Dealing with Identity Theft in Bankruptcy Cases*, 2001 Am. Bankr. Inst. J. 7 (Jan. 2001).

Kalama M. Lui-Kwan, *Article: VI. Business Law*, 14 Berkeley Tech. L.J. 463 (1999).

W. Everett Lupton, Comment, *The Digital Signature: Your Identity by the Numbers*, 6 Rich. J. L. & Tech. 10 (Fall 1999) (last visited 4/16/01) <http://www.richmond.edu/jolt/v6i2/note2.html>.

Charles R. Merrill & Robert J. Burger, *E-Quality at Last for E-Signatures: Statutory Changes Afoot May Finally Release E-Commerce from the Bonds of Ink and Paper*, N.J.L.J., Aug. 21, 2000, (last visited Apr. 16, 2001) <http://www5.law.com/nj-shl/display.cfm?id=3226>.

Raymond T. Nimmer, Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws (2000) (unpublished manuscript) (last visited Apr. 16, 2001) <http://www.bmck.com/ecommerce/topic-esignatures.htm>.

Joel Orr, *Identity Crisis*, 68 Civil Engineering, 52 (1998).

Kurt M. Saunders & Bruce Zucker, Essay, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 Cornell J.L. & Pub. Pol'y 661 (1999).

Kurt M. Saundersby, *The Regulation of Internet Encryption Technologies: Separating the Wheat From the Chaff*, 17 J. Marshall J. Computer & Info. L. 945 (1999).

Bruce Schneier, *Why Digital Signatures Are Not Signatures*, Crypto-Gram (last modified Nov. 15, 2000) <http://www.counterpane.com/crypto-gram-0011.html#1>.

Adam White Scoville, *Clear Signatures, Obscure Signs*, 17 Cardozo Arts & Ent. L.J. 345 (1999).

Peter Steiner, *"On the Internet, no one knows you're a dog,"* The New Yorker (pub. Jul. 5, 1993) (cartoon), (last visited Apr. 16, 2001) <http://www.cartoonbank.com/> and enter search terms "dog" and "cartoon".

John Udell, *Prove Identity With Digital Signature*, Byte.com (last modified Jul. 10, 2000) <http://www.byte.com/column/BYT20000706S0002>

Christopher B. Woods, *Commercial Law: Determining Repugnancy in an Electronic Age: Excluded Transactions Under Electronic Writing And Signature Legislation*, 52 Okla. L. Rev. 411 (1999).

Phil Zinkewicz, *The Push for Digital Signature Encryption: Will It Become Increasing Presence in the Insurance Industry?* 143 Rough Notes 52 (2000).