Richmond Journal of Law and Technology

Volume 6 | Issue 2 Article 7

1999

# The Digital Signature: Your Identity by the Numbers

W. Everett Lupton
*University of Richmond*

## Recommended Citation

W. E. Lupton, *The Digital Signature: Your Identity by the Numbers*, 6 Rich. J.L. & Tech 10 (1999).
Available at: http://scholarship.richmond.edu/jolt/vol6/iss2/7

Volume VI, Issue 2, Fall 1999

# The Digital Signature: Your Identity by the Numbers

**W. Everett Lupton** [*]

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

## Table of Contents

## I. INTRODUCTION

{1} Electronic commerce is the future of business. Today electronic commerce is a $3.6 billion industry. Thousands of businesses use the Internet to buy and sell their wares. As individuals and businesses increasingly use the Internet for commerce, contracts are moving online too. Because electronic commerce is conducted online, it is infeasible to make contracts through the traditional paper method. An electronic contract can be sent halfway across the world in seconds; whereas the same contract on paper would take days or weeks.

{2} The advantages of speed and convenience aside, electronic contracts must still meet the same legal requirements of traditional contracts. The contract is the same, but the difference is the medium in which the contract is embodied. Electronic and paper-based contracts have common elements, one of which is the requirement of a signature for contracts dealing with certain subjects.[1]

{3} What is a signature? A signature may be defined as "any mark made with the intention of authenticating the marked document."[2] Marks fulfilling this definition of "signature" have been used throughout history. For example, to make a contract under Roman law, a citizen pressed his signet ring into a *cena*, or tablet of wax.[3] During the Middle Ages, Europeans affixed a seal made of clay to a document; this seal "authenticated" the marked contract.[4] Later, parties to a contract began to write their signatures by hand in script.[5]

{4} Cryptography, the "art of secret writing,"[6] also has historical roots. People have used two basic forms of cryptography in centuries past: ciphers and codes.[7] Codes are lists of words used secretly to pass information;[8] whereas a cipher is a method of changing a letter, or group of letters, into "other letters, numbers, or symbols."[9] The ancient Spartans and the Romans both used a particular cipher.[10] Today, society usually uses ciphers rather than codes.[11]

{5} Electronic signatures present the latest embodiment of the signature and cipher. 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 of signatories. Some electronic signatures are very secure. A retinal scan, for example, is almost impossible to duplicate. Other electronic signatures provide for less security. For instance, a handwritten signature can be scanned, input into a personal computer and used to "sign" documents.

{6} One particular type of electronic signature that uses the principles of a cipher is the digital signature. The digital signature may be defined technically as:

> A transformation of a *message* using an *asymmetric cryptosystem* and a *hash function* such that a *person* having the initial *message* and the *signer's public key* can accurately determine:
>
> > (1) whether the transformation was created using the *private key* that *corresponds* to the *signer's public key*, and
> >
> > (2) whether the initial *message* has been altered since the transformation was made.[12]

{7} It is important to distinguish between a digital signature and other types of electronic signatures. A digital signature is not the same as an electronically-stored handwritten signature.[13] A digital signature is a secure communication unlike many other types of electronic signatures. Digital signatures ensure that contracts, images, letters, and many other forms of electronic documents can be signed and sent to another party within seconds without fear of compromise of security. The digitally signed contract is legally valid and can be read only by the intended recipient.

## II. ENCRYPTION AND THE TECHNICAL FRAMEWORK OF DIGITAL SIGNATURES

### A. *Knowing the ABCs: Algorithms, Bits, and Ciphertext*

{8} A digital signature is an electronic communication, which consists of "bits" of data. In its most fundamental state, a "bit" is a "0" or "1." Computers interpret these bits into strings of data, which are essentially a series of linked "0's" and "1's."[14] An electronic communication takes place when a computer transmits data in the form of bits[15] through metal or fiber-optic wires to another computer's microprocessor. The computer's microprocessor "translates" the numerical "string" into words and phrases. Thus, a digital signature is essentially a unique sequence of bits, created as an identifier of a certain message from a certain individual by a computer, and communicated via computer to another party.

{9} The science of encryption assures the security of a digitally signed message or document. There are, generally, two types of encryption: symmetric key cryptography and asymmetric cryptography, otherwise known as public-key encryption ("PKE").[16] Digital signatures are formed through PKE. The framework of PKE services is commonly known as a public key infrastructure ("PKI").[17] PKE technology manipulates data into numerical digests and vice-versa,[18] with algorithms as the key mechanisms used to manipulate the data.[19] "Schemes" are particular algorithms, or series of algorithms, used to manipulate data in digital signature technology.[20] One of the most common schemes currently used in PKE is the RSA scheme.[21]

{10} The basic operation behind this scheme is the use of a "key" as an exponent that is applied mathematically to the number representing the message.[22] The message in its initial, or numerical, state is called "plaintext."[23] The number resulting from the enciphering process is called the "ciphertext."[24] In the RSA scheme, the ciphertext is a number that is mathematically manipulated with some other random number by an algorithm; this "other" number is also needed as part of the key.[25] Together, the two numbers form the private key.[26] The other number formed as a result of the applied algorithm is a part of the public key[27] and is used to decipher the ciphertext and to recreate the original plaintext message. At this point, a practical consideration to make is that the number of digits in one or more of the numbers comprising the ciphertext must be large enough to defeat attempts to "hack," or to find the private key to the message.[28] If the process is followed precisely, the hacker would have to go through each and every possible combination, permutation, and algorithm to decipher the number.[29]

### B. *Hashing*

{11} Hashing is another technical process used to make a digital signature.[30] Hashing refers to the process of creating a string of characters, also called a digest, by mapping from the full plain-text message (i.e., the use of an algorithm).[31] The algorithm used to form the digest from the plaintext message is usually designed with the seal function in mind.[32] Thus, if any character in a digitally signed message is changed, the digest also changes. Throughout the process, it is essential that each individual plaintext message results in a single, unique digest.[33] Typically, each digest is compiled in a fixed length in a size small enough to be enciphered as the message substitute in the construction of the actual digital signature with the private key.[34] This compilation allows a very large plaintext message to be represented in the digital signature formation by a short string that is known to the user or the user's digital signature software.[35]

{12} To decipher the message, the recipient must know the hashing algorithm.[36] The hashing algorithm is applied to the full plaintext part of the received message. It is this process that results in a digest.[37] The resulting digest is then used to verify the digital signature. As previously stated, if even one bit has been changed since the message was signed, the signature will not be verified.[38]

{13} The authentication of a digital signature using PKE is important. In order to rely on a PKE-signed message, the receiver must be able to associate the public key with the sender/author.[39] Handwritten signatures are readily identifiable with an individual, as each person's signature is unique. However, digital signatures are essentially large numbers, which appear to be an algorithm to the ordinary observer. A digital signature does not contain any handwriting or other unique properties that can be readily associated with a particular individual. Thus, a digital signature must be associated with an individual to be effective.

### C. *Verification and the Role of Certification Authorities as Trusted Third Parties*

{14} This association of a digital signature with an individual's identity must also be verified. Utilizing current asymmetric encryption technology, such as digital signature software, anyone can create a public key-private key pair in the name of any particular person.[40] In other words, anyone can download digital signature software from the Net and create a digital signature for "Joe C. Smith." The signature can even be uploaded to certain databases of public keys.[41] But, how does anyone confirm that the individual who created the key is "Joe C. Smith?" Without independent verification, the public key of Joe C. Smith may be a fraud perpetrated by another individual purporting to be Joe C. Smith. Consequently, a receiving party may rely unknowingly on a fraudulent signature. Therefore, digitally signed messages purporting to be associated with an individual identity should be attested to by a trusted third party ("TTP") to minimize the occurrences of fraudulent representations.

{15} Certification authorities ("CAs") are the most common way to provide this authentication. A CA is a TTP that acts as a repository of public keys and authenticates the relationship between a particular public key and its supplier.[42] The CA must ascertain the true identity of the subscriber and certify that a public key-private key pair belongs to that person.[43] First, the subscriber must generate her own public key-private key pair. The subscriber then visits the CA and produces proof of identity. Most CAs require an official document with picture identification, such as a driver's license and/or passport.[44] Finally, the CA will require a demonstration that the subscriber holds the private key corresponding to the public key.[45] This demonstration is difficult because the key owner cannot disclose the private key.[46] One way of accomplishing this is by sending a digitally signed electronic message in the presence of the CA.[47]

{16} A certificate is issued by the CA upon verification of the association between an identified person and public key.[48] A certificate is an electronically stored record attesting to the connection between the public key and subscriber.[49] The certificate also contains the subscriber's public key and may contain other relevant information, such as the key expiration date,[50] size, and/or signature generation software identifier.[51] According to the ABA's *Digital Signature Guidelines*, a CA

> may give notice of the creation and contents of a certificate by giving the subscriber 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.[52]

Generally, the CA is not required generally to publish a certificate upon its issuance.[53] The CA does, however, attach its own digital signature to the certificate if it is sent electronically.[54] The subscriber must then review the contents of the certificate to ensure accuracy before the certificate is made publicly available.[55] The subscriber must accept the certificate for both verification and validation.[56] After the subscriber has reviewed the contents of the certificate and is certain of the certificate's accuracy, she "may *publish* the certificate, or direct the CA to do so. . . ."[57] Once the CA publishes the certificate, it represents that the certificate has been accepted by the subscriber, and the certificate is given a presumption of validity.[58]

{17} 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.[59] A repository is "an electronic database of certificates - the equivalent of [an online] digital Yellow Pages" accessible to the general public.[60] However, unlike the Yellow Pages, a user may be charged for access to the information.[61]

{18} A private key, like a physical key, must be physically safe guarded. If a private key becomes known to another party, the security of all communications using that private key is compromised. When the private key is either lost or compromised, the individual should suspend or revoke the certificate corresponding to the key-pair immediately. The certificates stored at a repository usually contain the status of the certificate, such as whether the certificate is "valid," "suspended," or "revoked."[62] 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.[63]

{19} A CA may be liable for negligence in performing its functions or for misrepresentation in the issuance of certificates containing false or misleading information.[64] The CA may also be liable for breach of contract between the CA and the subscriber. Statutory provisions may limit the liability of a CA, depending upon the relevant jurisdiction.[65] If a statute is inapplicable, a CA may attempt to mitigate potential liability by specifying a limit in its contract with a subscriber.[66] A CA's certification practice statement often contains a disclaimer of liability.[67] The CA will claim usually that this disclaimer limits any potential liability to a third party who relies on a certificate issued by the CA.[68] This notification of limitation may be enforceable when a CA defends itself against a relying party, depending, in part, on whether the relying party had notice of the CA's limitation of liability disclaimer.[69]

## III. THE LEGAL FRAMEWORK

### A. *The Functions of a PKI Digital Signature*

#### 1. Integrity, Authenticity, and Verification

{20} The digital signature, like a handwritten signature, fulfills certain legal roles. First, a digital signature assures the integrity of a communication. Digitally signing the message ensures that the contents of the message are concealed and secure.[70] As previously mentioned,[71] a document that is in any way altered after it has been digitally signed using public key encryption will be unverifiable. This is particularly applicable in situations where an author is required to prove at a later date that the intended recipient of the communication did not alter the message after its receipt.

{21} Authenticity is another function of a digital signature. A connection between the digitally signed document and signer must be shown. Digital signatures provide a significantly greater reliability of authenticity than conventional, hand-signed documents, because of the mathematical improbability of forgery.[72] A CA is the TTP that provides the verification of the link between public key and signer identity.[73]

{22} Yet, a question remains: how can the identity and authority of the CA be verified? One way to verify an issuing authority, such as a CA is certification by another "higher-level" CA. This hierarchy of verification can continue until a certain point, and then must logically end with a "final" CA. This "final" CA must be well-known and highly trusted by commercial entities.[74]

{23} What is required of a CA? The ABA's *Digital Signature Guidelines* establishes a model legal structure for CAs.[75] The Guidelines state that, "[s]ubject to applicable law, any person who undertakes the functions of a certification authority . . . may become a certification authority."[76] The Guidelines further specify that the authority and reliance accorded the certificate of a CA is determined by the CA's experience and reputation, as well as by material contained within a certification practice statement.[77] A second method of CA verification is by statute, such as the Utah Digital Signature Act.[78] Many digital signature statutes list certain issuing authorities as official CAs.[79]

{24} Another function of a digital signature is the seal function. A digital signature performs the seal function either through the "hash function"[80] or by enciphering the entire plaintext message,[81] and verifies that the message has not changed since the sender's private key signed the message. The sender of the digitally signed message is assured that the recipient cannot modify the message because the recipient only has access to the sender's public key. Throughout the entire transaction, the private key is never disclosed. Conversely, the recipient is assured that the message has not been intercepted and modified by a third party.[82] If, at a later date, a party needs to produce a copy of the message, a verification of the digital signature will confirm that the message remains preserved, uncorrupted, and, therefore, unmodified.[83] This means that a party can produce a digitally signed communication in court and establish that the document is prima facie valid.

#### 2. Non-Repudiation

{25} Another function of a digital signature is the presumption of non-repudiation. When the author/sender of the document affixes her signature to the message, she is presumed to intend to authenticate the document with all of the accompanying rights and duties.[84] An attempt by the signatory of a digitally signed document to repudiate her authentication, or her intent to do so, is more difficult than an attempt to repudiate a hand-signed document, as it is highly improbable that anyone other than the signatory could have signed and sent the digitally signed document. The physical security of PKE technology means that the document must have been signed with the sender's/signatory's private key.[85]

{26} It is theoretically possible for another party to discover a private key, even though the key's holder has conscientiously safeguarded it. The key may be broken through a "brute force" attack. In such an attack, every possible key is tried until the correct key decrypts the ciphertext.[86] The longer the key, the less the probability of a successful brute force attack. The length of the key is directly proportional to the amount of time required to break that key. For example, a 56-bit long key would take approximately ten hours to break in a brute force attack,[87] whereas a 128-bit long key would take 5.4 multiplied by 10^18 years to break.[88]

{27} The only viable defense to a cause of action for breach of contract is the forgery of the digital signature owner's identity. According to the ABA's *Digital Signature Guidelines,* if the owner's private key has been compromised or lost, the "forger" has signed on his behalf only.[89] The owner of the signature, nevertheless, is legally presumed to have signed a message if the owner is a "subscriber of a valid certificate, and the digital signature can be verified by reference to a public key listed in the certificate . . . ."[90] This presumption may be rebutted upon a showing of sufficient evidence.[91] The subscriber, furthermore, has a duty to notify promptly, "upon reasonable suspicion" any CAs holding a public key corresponding to the compromised or suspect private key.[92] Additionally, it is important to determine whether the alleged signatory intentionally disclosed his/her private key. The *Digital Signature Guidelines* differentiate between intentional and accidental disclosure of a private key: "[p]ersons who intentionally discloses [sic] their private keys, *with or without fraudulent intent,* should be held to a higher standard [of care] than an involuntary discloser."[93]

#### 3. Ceremony

{28} Another function of a digital signature is the ceremonial function. At least one expert, however, believes that a document is more likely to be signed accidentally with the digital signature than with a traditional handwritten signature.[94] Yet, regardless of a digital signature's ease of use, a standard of reasonable care for an individual's private key is necessary to preserve the ceremonial function of a digital signature.[95] Therefore, the ABA *Digital Signature Guidelines* establish a presumption of intent to affix one's signature.[96] This presumption, nevertheless, may be rebutted by a sufficient evidentiary showing.[97] The result of such a presumption is that, in cases of an "accidental" signing, the individual is required to show evidence that the signing was indeed an accident. Because it will be difficult for the signer to meet the requisite burden of proving accident, the signer should exercise great care to avoid such an accidental signing.

{29} There are several safeguards an individual can undertake to decrease the probability of accidental signing. Private keys are stored usually on a computer's fixed disk or hard drive in a folder called a "key-ring."[98] By removing all private keys to a remote device, such as a floppy diskette or magnetic card, an individual is required to perform several distinct actions to digitally sign a document, thereby significantly reducing the likelihood of accidental signing.

### B. *Evidentiary Issues*

{30} Despite the many advantages of digital signatures, they lack several important features. For example, the lack of a built-in, verifiable time/date stamp is a flaw in current digital signature technology. Although a digitally signed message is dated at the moment of sending, the date and time can be manipulated easily, and therefore, are untrustworthy.[99] The only currently available method for verifying a digital signature is an independent time/date stamp from a CA.[100] The CA must first verify the time and date the message was received from the subscriber. The CA then forwards the message with the time/date stamp to the intended recipient.[101]

{31} Although even this method of CA verification can present problems. One implication of the inability to ensure an accurate date/time stamp on a digitally signed message is the difficulty in proving the exact time the message was sent. A CA's date/time stamp only shows when the message was received from the subscriber. Thus, a party relying upon the date/time stamp of the CA can only prove that the message was sent by the subscriber at some date or time prior to date or time stamped on the message. A litigant attempting to prove the exact time the message was signed by the author would have to rely upon extrinsic evidence.[102]

{32} The use of a digital signature in commerce, like a handwritten signature, is subject to the Uniform Commercial Code,[103] Statute of Frauds,[104] and the Parol Evidence Rule.[105] Under the laws of most states, the common law forms for assigning real property have been superceded by statutory forms for deeds.[106] Therefore, the formal requirements of a signed writing needed to accompany an assignment of real property have a legal basis separate from the Statute of Frauds.[107] The ABA *Digital Signature Guidelines* do not address the possibility of circumventing the statutory deed signing requirement through the use of a digital signature.[108] Because a digital signature satisfies, and to some extent exceeds,[109] the requirements of a traditional signature, future statutory amendments should authorize the use of digital signatures in real property assignments.

{33} The Parol Evidence Rule allows courts to consider evidence (i.e., digital signatures) beyond that found in the contract in some situations.[110] Under the Parol Evidence Rule, extrinsic evidence is deemed inadmissible to effect a determination of the intention of the subscribing parties in their contract.[111] A digitally signed document can satisfy two requirements. First, a digitally signed document satisfies the "writing" requirement.[112] Secondly, a digital signature may authenticate the document.[113]

{34} Another evidentiary application of digital signatures is the Best Evidence Rule.[114] The Federal Rules of Evidence expressly provide that, "[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original."[115] Although an electronic message is authenticated, a party must still overcome the hearsay rule if it is to be admissible.[116] It is also necessary to survive hearsay objections, as electronic messages may themselves constitute hearsay (i.e., hearsay within hearsay).[117] Additionally, the message itself may contain references to statements that are hearsay. A party may find an applicable hearsay exception that will admit the electronic communication as evidence for the jury's consideration. One such example is the Business Records Exception,[118] which is applicable to electronic communications used in the regular course of business. A computer record will be admissible generally under this exception if it was the regular business practice to create the computer information.[119] However, if the court finds that the source of the information, method, or circumstances of the preparation indicate a lack of veracity, the record(s) will be excluded.[120] Thus, there is no reason why a digitally signed electronic document should be treated differently than other types of business records.[121]

## IV. A SURVEY OF ELECTRONIC SIGNATURE LEGISLATION

### A. *Legislative Categorization: Neutrality, Neutrality Plus, and PKI-Technology*

{35} There are various legal structures for digital signatures. Since the enactment of the Utah Digital Signature Act,[122] more than forty states have enacted some form of electronic signature legislation.[123] The types of legislation differ from state to state. Nevertheless, current state electronic signature laws may be classified into three general categories. The first category of statutes are "technology neutral."[124] These statutes give legal effect to any electronic signature, but they allow a court to decide what evidentiary weight to give the signature based upon the security of the technology utilized. The second category of statutes specifies that a valid signature must have certain security attributes, but does not require a particular technology. Such statutes tend to require the attributes of PKI-digital signatures, such as user authentication and message-alteration prevention.[125] The third group of statutes requires the use of PKI-digital signatures.[126]

{36} The following illustrations present the electronic signature laws of three states, with each state's statutes adopting one of the three available approaches. Utah, for example, has adopted the third approach. The Utah Digital Signature Act ("Utah Act") was the first comprehensive statute on digital signatures.[127] The Utah Act established specific duties of CAs and subscribers,[128] license and regulation procedures for certification authorities,[129] legal presumptions on parties,[130] and the legal validity of digitally signed documents.[131] Many of the provisions of the Utah Act were later adopted by the ABA in its *Digital Signature Guidelines*.[132]

{37} California, however, has adopted the second approach. The California Digital Signature regulations[133] are not as detailed as the Utah Act. The California regulations define a "digitally signed communication" as "a message that has been processed by a computer in such a manner that ties the message to the individual that signed the message."[134] Currently, California recognizes two digital signature technologies: public key cryptography and "signature dynamics."[135] The regulations also provide a procedure for adding new technologies to the list of acceptable technologies. With respect to digital signatures, the California regulations impose the duty to exercise reasonable care in retaining control of the private key, and preventing its disclosure to any person not authorized to create the subscriber's digital signature upon all persons who hold key pairs.[136] Comparable to the Utah Digital Signature Act, the California regulations also establish an approved list of CAs authorized to issue certificates for digitally signed communications with public entities in California. To qualify as an approved CA, an applicant must undergo a thorough audit.[137] A CA may avoid the audit by providing proof of accreditation by a national or international accreditation body that is deemed acceptable to the State of California.[138] It is significant to note, however, that the California regulations do not specifically address liability concerns. The legislative commentary for the regulations suggest remedies in the form of contractual provisions with service providers. The California legislature is expected to establish additional sections dealing with liability.[139] Currently several additional digital signature bills are pending in the California Assembly.

{38} In contrast, the Commonwealth of Virginia takes the least technology-specific approach. The Virginia provisions employ "technology-neutral language."[140] Virginia Code Sections 59.1-467 and 59.1-468, define "digital signature" as "any electronic identifier, created by a computer" and "signed" as "any symbol or method . . . adopted by a party with present intention to be bound by or to authenticate a record. . . ."[141] Section 59.1-468 grants full legal effect to digital signatures: "[w]here law requires a signature, or provides for certain consequences in the absence of a signature, that law is satisfied by a digital signature."[142]

### B. *Attempts for a Uniform Digital Signature Law*

#### 1. U.S. Proposals

{39} Because each state has a different law on electronic signatures, some groups are attempting to unify and to standardize the various laws into a uniform law. The National Conference of Commissioners on Uniform State Laws (NCCUSL) and the American Law Institute ("ALI") have promulgated separately two "model laws" addressing electronic signatures, the Uniform Electronic Transactions Act ("UETA") and the Uniform Computer Information Act ("UCITA").[143]

{40} Although primarily addressing licensing aspects of information transactions, UCITA encourages the implementation of digital signatures. The provisions of UCITA do not favor digital signatures over electronic signatures.[144] In fact, UCITA does not attempt to override the existing laws of individual states, as it leaves existing provisions intact. Despite the fact that UCITA provides a model law for software licensing, an area that currently has very little relevant legislation, the prospects for UCITA appear dim because there are significant issues of consumer protection and federal preemption that have not been adequately addressed.[145]

{41} In addition, Congress is also weighing in on digital signatures. Currently, there are several major bills in Congress addressing digital signatures.[146] In 1999, two important bills were introduced in the House of Representatives. The Digital Signature Act of 1999[147] and the Electronic Signatures in Global and National Commerce Act[148] are "national" digital signature bills. Both require the "adoption and utilization of digital signatures by Federal agencies and ... encourage the use of digital signatures in private sector electronic transactions." Under the Digital Signature Act of 1999, federal agencies would be required to allow digital signatures in place of a written signature. Both bills, furthermore, would establish several "panels" to study and to encourage the use of digital signatures. Both bills are still pending before the House Commerce Committee.[149]

### 2. International Initiatives

{42} Therefore, it should come as no surprise that there are also various international provisions relating to digital signatures. Digital signatures are particularly attractive to parties engaged in international electronic commerce. The distances and physical barriers between states such as border patrols, customs, and oceans are significantly diminished through electronic communication. Many countries are exploiting the full advantages of these communication tools - digital signatures. For example, Argentina, Australia, Canada, Colombia, Denmark, France, Germany, Ireland, Italy, Japan, Malaysia, the Netherlands, Russia, Singapore, Sweden, and the United Kingdom all have some form of enacted or pending digital signature legislation.[150]

{43} The European Union ("EU") also has established a framework for electronic and digital signatures.[151] On May 13, 1998, the European Commission released its report for a "Directive of Digital and Electronic Signatures" ("Directive").[152] In its report, the Commission recognized the increasing amount of digital signature legislation in member states of the EU, as well as the need for a uniform legal structure in the "Internal Market" for digital signatures.[153] Additionally, the Commission recommended technology-neutral standards.[154] The Commission differentiated between closed and open systems, where the closed commerce systems would be specifically excluded from the coverage of the Directive.[155]

{44} The primary focus of the EU Directive was unifying the divergent initiatives in the EU member states.[156] Divergence was particularly evident in regards to requirements on service providers and products, the condition under which electronic signatures will have legal effect, and structure of accreditation schemes.[157] Other problematic areas in which the Commission urged expedient "harmonization" were the different liability rules and the risk of uncertain jurisdiction concerning liability, where services are provided among different member states.[158] According to the Commission, "[i]t also seem[ed] likely that Member States [would] set up different technical conditions under which electronic signatures will be presumed secure."[159]

{45} The EU Directive, in addition, establishes a legal framework for electronic signatures.[160] "Certification Service Providers" would offer their services without being required to obtain prior authorization from a Member State's government.[161] Service providers may benefit from the legal validity granted to the "associated electronic signatures" through "voluntary accreditation schemes linked to common requirements."[162] Any accreditation, accordingly, would be regarded as a public service offered for certification service providers which would like to provide high-level services.[163] Through the implementation of these policies, service providers will be able to take advantage of this new type of accreditation.

{46} The EU Directive also encourages certification service providers to offer a much wider range of services than a CA in the United States.[164] Certificates may include name, address, social-security number, tax and credit information, and specific licenses/ certifications.[165] Key concepts throughout the EU Directive are flexibility and standardization across borders.

{47} The EU Directive has been "fleshed out" by a subsequent study by European industry and standardization bodies. In its Final Report, the European Electronic Signature Standardization Initiative Expert Team set out "detailed standards and open specifications" for electronic signatures.[166] Instead of recommending or developing new standards, the EESSI Report urges the EU and its member states to use existing "recognized international standards."[167] Specifically, the EESSI Report establishes digital signatures using asymmetric cryptography (i.e., PKI-digital signatures) as the technical framework. In essence, the Report, although expressly stating a "technology neutral approach," favors asymmetric cryptography as the "first set" technology for "qualified electronic signatures."[168] The Report specifically addresses the establishment of profiles for PKI operational management protocols based on a specific PKI technology.[169] Thus, products using PKI-digital signatures would obtain the status and legal rights granted to "qualified electronic signatures."

{48} The United Nations ("UN") is also developing an electronic signature framework. The UN General Assembly adopted a Model Law on Electronic Commerce ("Model Law") in 1996.[170] Since 1997, the United Nations Commission on International Trade Law ("UNCITRAL") has worked on Draft Uniform Rules for Electronic Signatures ("Draft Uniform Rules"), a set of model rules for homogeneity in international commerce.[171] Most of the terms enumerated within the Draft Uniform Rules are defined according to the Model Law.[172] Although the latest proposal of the Draft Uniform Rules[173] contains diverse sections from various nations, the Draft Uniform Rules employ certain principals, one of which is "media-neutrality."[174] Specifically excluding administrative, consumer, and criminal law, and public policy,[175] the Draft Uniform Rules are specifically limited in scope to private international commercial law.[176] The Draft Uniform Rules propose that parties consider a type of parol evidence, such as custom of the parties or custom of the trade, in the reliance receiving parties place in the authenticity of certificates.[177] The *Draft Uniform Rules* provide three variants, all of which basically establish a "presumption of signing" if "an enhanced digital signature is attached or logically associated with the data message," reserving two cases in which the presumption does not apply[178] and yielding several "variants" for establishing liability.[179] Section III of the Draft Uniform Rules establishes general standards of practice for certification authorities.[180] Additionally, the Draft Uniform Rules set forth a presumption of integrity for digitally signed messages.[181] Finally, Articles Eleven and Twelve establish contractual liabilities on certification authorities.[182]

{49} A review of each article of the Draft Rules reveals an astonishing similarity to the ABA's Digital Signature Guidelines.[183] Although the Draft Rules differ in specific terminology (e.g., "enhanced electronic signature" rather than "digital signature"), the basic legal frameworks of the two proposals are quite similar. The refutable presumptions of authenticity and integrity and the reliance upon certification authorities are but two examples of the similarity between the UN's Draft Uniform Rules and the ABA's *Digital Signature Guidelines*.

## V. Conclusion

{50} The digital signature has become a significant tool in U.S. and international commerce. Because a digital signature provides the legal elements of a traditional handwritten signature (i.e., evidence, ceremony, approval, and efficiency) and enhanced security, integrity, and authenticity, additional businesses will likely use digital signatures in an increasing percentage of their commercial transactions. Secure electronic commerce provides a "paperless" way of transacting business.

{51} Electronic communications may be sent and received in a fraction of the time, as compared with traditional methods. A digitally signed contract may be e-mailed from a business in Beijing to a recipient in New York in less than one minute, while the same document could take a day (or even longer) to arrive if sent through a commercial delivery service. The very small amount of time required to send a digitally signed message to a recipient, as previously examined, has broad implications on the law of contracts. In short, the digital signature is the means to an end; a signature is not part of a transaction's substance, but rather, the authentication of a transaction.[184]

{52} Currently, the PKI-digital signature is the best type of signature for electronic contracts. PKI-digital signature software is inexpensive and the technology is mathematically improbable to break.[185] With future advances in technology, other types of electronic signatures may replace the PKI-digital signature. Regardless of the technology used, digital and electronic signatures are an increasingly significant part of commerce and will continue to evolve.

*-W. Everett Lupton*

[*] W. Everett Lupton earned his B.S. in Business Administration from Old Dominion University in 1997. He will receive his J.D. from the University of Richmond School of Law in 2000. Mr. Lupton is currently the Technical Editor of the *Richmond Journal of Law & Technology*. He is also a member of the Moot Court Board and Trial Advocacy Board. The author would like to thank Professors Tim Coggins and Deborah Tussey for their critical review of his work.

[1]. *See* RESTATEMENT (SECOND) OF CONTRACTS Section 131(1978); *see also* U.C.C. Section 1-201(39) (1998).

[2]. *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, 1996 A.B.A. INFO. SEC. COMM. 3 [hereinafter *Digital Signature Guidelines*] (citing U.C.C. Section 1-201(39) (1992)).

[3]. *See* Jacqueline O'Neal, *The Notary: Yesterday, Today, and Tomorrow* (visited Oct. 11, 1999) <http://www.lna.org/l_esprit/oneal.htm>.

[4]. *See id*.

[5]. *See id*.

[6]. BERT-JAAP KOOPS, THE CRYPTO CONTROVERSY: A KEY CONFLICT IN THE INFORMATION SOCIETY 33 (1999).

[7]. *See id*. at 34.

[8]. *See id*.

[9]. *Id*.

[10]. *See id*.

[11]. *See id*.

[12]. *Digital Signature Guidelines*, *supra* note 2, at 35 (emphasis in original).

[13]. European entities sometimes use the term "electronic signature" in place of "digital signature." *See, e.g.*, McBride, Baker & Coles, *Summary of Electronic Commerce and Digital Signature Legislation, European Union* (visited Sept. 10, 1999) <http://www.mbc.com/ecommerce/legis/eu.html#EUROPEAN COMMISSION 297>.

[14]. These "01" or "10" sequences are commonly referred to as hex-decimal code, a machine language.

[15]. 1,000 Bits = 1Byte; 1,000 Bytes = 1KB; 1,000KB = 1MB, etc.

[16]. *See* Michelle Jolicoeur, *Digital Signatures: The Key to Information Technology Security* (visited Sept. 10, 1999) <http://www.govtech.net/publications/gt/1998/may/storyc/storyc.shtm>.

[17]. *See* KOOPS, *supra* note 6, at 45.

[18]. *See id*. at 34-35 (discussing the process of cryptography).

[19]. *See* Lawrence Pinsky, *Digital Signatures: A Sign of the Times* (visited Sept. 19, 1999) <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>. Dr. Pinsky's paper provides a more detailed explanation of the mathematical processes used in digital signature encryption.

[20]. *See id*.

[21]. *See* KOOPS, *supra* note 6, at 37.

[22]. *See* Pinsky, *supra* note 19 <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>.

[23]. *See* KOOPS, *supra* note 6, at 35 (defining plaintext message as "[a] clear message").

[24]. *See id*.

[25]. *See* Pinsky, *supra* note 19 <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>.

[26]. Unlike symmetric key systems, public key encryption uses two keys, one widely-distributed "public" key and another secret "private" key. *See* KOOPS, *supra* note 6, at 36.

[27]. Public keys are of varying lengths. The following is the author's public key and may serve as an example of a 3072/1024 bit PKE/RSA generated key:

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: PGP Personal Privacy 6.5.1

mQGiBDZbWB0RBADvPvhVwh6H5B5DHnZ/XKgvdkkdnaOXazOSVmR6Z+6azFcQi3HnVGqCl19clxnxCbMU0m5+sBQ+UCQLP2umdvhIGRZafgqpMYWODpBd4kZCVb
TjfjVYt/prT4XyeM8/GPtzM4T5aDnCesq7qK3+XT79np7zsydlL3XuN19QCg/9ijg3/6/EddkK5YjoQdaR37xtkD/j3xZ/Mj4w5HwLD25S44LWQ6Gkj54VPTnBfFt7MT
kvVS8/ri0jzHE46mG5AR6fr9aksMd6wNqjptOwrP+Afgrf8YNXOMZlj1Yrr7KevtQz0Qxw/ke8pTtIUcjcuUzjSFQizzL48CqrjzhPvFtiIvUFEkMoyc+CoYpXJBHIM+
cP9xA/98e6J+BVwSsxQA+gqtOAPyUw/cu04QgYuQklZeWHtk1qA+MaEX2M2AQO5aw8jquBRfRu1vO4UZ/zcRHT9+FVTy8DZAfzZP7MsS/LyN3VZraBIz7jsSFNF108UO
YkTUBcii8sx0uoOGp5IH5EiTCfARmaNqSdAhQ/yOs0hwFeDTf7QpV2FsdG9uIEV2ZXJldHQgTHVwdG9uIDxsdXB0b25AYWJhbmV0Lm9yZz6JAEsEEBECAAsFAjZbWB0
AZ5GGUQSrqpYwqQWgfy0KFcuIEV2ZXJldHQgTHVwdG9uIDx3bHVwdG9uQHJpY2ht
b25kLmVkdT6JAEsEEBECAAsFAjZwh8gECwMCAQAKCRAGN3KEFhdsH9IPAJ93+hTW
EtC+7MmiLibmZkKUeD9jpgCdHEPtUx1YQ0gMisR8H0BBDCgWymW5Aw0ENltYHxAMAMwdd1ckOErixPDojhNnl06SE2H22+slDhf99pj3yHx5sHIdOHX79sFzxIMRJitD
YMPj6NYK/aEoJguuqa6zZQ+iAFMBoHzWq6MSHvoPKs4fdIRPyvMX86RA6dfSd7ZC LQI2wSbLaF6dfJgJCo1+Le3kXXn11JJPmxiO/CqnS3wy9kJXtwh/CBdyorrWqULz
Bej5UxE5T7bxbrlLOCDaAadWoxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHT UPj1WV/cdlJPPT2N286Z4VeSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq
01uejaClcjrUGvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O
9vPJI8BD8KVbGI2Ou1WMuF040zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcK
ctaGxAMZyAcpesqVDNmWn6vQClCbAkbTCD1mpF1Bn5x8vYlLIhkmuquiXsNV6Uwy
bwACAgv+Lr1Uy6Rco363CZaCztX92uFHQUlbG1XNKt2a3WJfAc4BRB5xGukdIRR+
FMqSQ4q8rNjJCBUPECVk9Mtwbjp8LTiS+VSfwPZzcEJmivghnoc2veMHGhdQuRue
hajDQUuGutiKkZ0PDvPNHO76Cxd8y7254h8M9J/BYE0EItdE7HuhFRWXUsssWrLD
PJBbkPMO8NAap23Cb+TX94RZStonpMSi6+29dgWjW/isusBHTQiBCaXX7XlhAps0 B3Chmnmcegb4u8qq3/GUgyp4oeJPjFXYQAjzN+QxElN/8QOPnu0ekkDdXYCPXjnv

gkbbTEmnVvTsVbbKFtx8Eeau+VwKMRuNJN5yN8MZs+haVSqYWZToQvv03nbceKtf
ygztuE9ZMf0QA2+wDNpWnwftWOBK3701jfHzG0qh6wJtB+wJ60c1dXdudStm9YuX q6fYJaySxj91OX2AePZTJwx7yh7KTDKhwlVklo/GOMFM7Ldj750WI3b3lTm4xiZk
kc9kjZRyiQBGBBgRAgAGBQI2W1gfAAoJEAY3coQWF2wfuHAAn0Devuz1FOAx5p4z ozYv6OvEfYkyAJ4nEiqDNO/ZwIn5spN8wf/p/6HfAg===7am6

-----END PGP PUBLIC KEY BLOCK-----

[28]. *See* KOOPS, *supra* note 6, at 42.

[29]. *See* Pinsky, *supra* note 19 <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTML>; KOOPS, *supra* note 6, at 42.

[30]. *See* KOOPS, *supra* note 6, at 38-39.

[31]. *See* Pinsky, *supra* note 19 <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>.

[32]. *See* KOOPS*, supra* note 6, at 38-39.

[33]. *See* Pinsky, *supra* note 19 <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>.

[34]. *See* KOOPS, *supra* note 6, at 38.

[35]. *See* Pinsky, *supra* note 19 <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>.

[36]. *See* KOOPS, *supra* note 6, at 36.

[37]. *See* Pinsky, *supra* note 19 <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>.

[38]. *See id*.

[39]. *See* KOOPS, *supra* note 6, at 39.

[40]. *See* THOMAS J. SMEDINGHOFF, ET AL., ONLINE LAW: THE SPA'S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET 46 (Thomas J. Smedinghoff ed., 1996); *see also* KOOPS*, supra* note 6, at 55 n.45.

[41]. One such database is a repository. *See infra* note 59 and accompanying text.

[42]. *See* SMEDINGHOFF, *supra* note 40, at 47.

[43]. *See id*.

[44]. *See id*.; *see also VeriSign Certification Practice Statement* 38-42 (visited Oct. 2, 1999) <http://www.verisign.com/repository/CPS/index.html>.

[45]. *See* SMEDINGHOFF, *supra* note 40, at 47.

[46]. *See id*.

[47]. *See id*.

[48]. *See id*.

[49]. *See id*.*; see also Digital Signature Guidelines*, *supra* note 2, at 29.

[50]. *See* SMEDINGHOFF, *supra* note 40, at 47.

[51]. A signature generation software identifier is a small amount of text identifying the particular software vendor and version. For example, the public key at Endnote 27 identifies the generating software as "PGP Personal Privacy 6.5.1".

[52]. *Digital Signature Guidelines, supra* note 2, at 40.

[53]. *See id*. at 41.

[54]. *See* SMEDINGHOFF, *supra* note 40, at 47.

[55]. *See id*.

[56]. *See Digital Signature Guidelines*, *supra* note 2, at 41.

[57]. *See* SMEDINGHOFF, *supra* note 40, at 47 (emphasis in original).

[58]. *See Digital Signature Guidelines*, *supra* note 2, at 41.

[59]. *See id*. at 47.

[60]. SMEDINGHOFF, *supra* note 40, at 47; *see also Digital Signature Guidelines*, *supra* note 2, at 48-49.

[61]. *See Digital Signature Guidelines, supra* note 2, at 49.

[62]. *See id*.

[63]. *See* SMEDINGHOFF, *supra* note 40, at 50.

[64]. *See Digital Signature Guidelines*, *supra* note 2, at 68-69, 79.

[65]. *See* SMEDINGHOFF, *supra* note 40, at 50-51.

[66]. *See id*. at 51.

[67]. *See id*.

[68]. *See id*. at 51; *see also Digital Signature Guidelines*, *supra* note 2, at 33.

[69]. *See Digital Signature Guidelines*, *supra* note 2, at 33.

[70]. *See* Tyson Macaulay, *Conventional Encryption No Longer Enough,* 25 COMPUTING CANADA 35, Sept. 17, 1999 (visited Feb. 25, 2000) <http://www.plesman.com/cc/>.

[71]. *See* discussion *supra* at note 32.

[72]. *See* Pinsky, *supra* note 19, at Part III <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>.

[73]. *See supra* text accompanying notes 42-45.

[74]. *See generally* SMEDINGHOFF, *supra* note 40, at 49 (noting the recipient of a message may trace certificates issued by CAs "up the chain until reaching a certificate issued by a CA he or she knows and trusts).

[75]. *But see* Edward D. Kania*, The ABA Digital Signature Guidelines: An Imperfect Solution to Digital Signatures on the Internet*, 7 COMMLAW CONSPECTUS 297, 306-13 (1999) (discussing some potential technical problems encountered when implementing the subscriber - certification authority - recipient process).

[76]. *Digital Signature Guidelines, supra* note 2, at 31.

[77]. *See id*. The Guidelines specifically mention CyberNotaries as a level certification authority. *See id*. A CyberNotary is a lawyer admitted to practice within the United States and certified by the ABA. A CyberNotary would, additionally, be required to show "technical competence in computer-based business transactions." *Id*. Under the planned specialization rules, a CyberNotary would primarily handle international electronic commerce transactions. *See id*.

[78]. *See* UTAH CODE ANN. Sections 46-3-101 to 46-3-504 (1999).

[79]. *See id*.; California Digital Signature Act, CAL. GOV'T CODE Section 16.5 (West 1999), CAL. CODE REGS. tit. ii, Sections 22000-22005 (1998); Virginia Digital Signatures Act, VA. CODE ANN. Sections 2.1-563.13, 59.1-468, 59.1-469 (Michie 1999).

[80]. *See supra* note 31 and accompanying text.

[81]. *See supra* note 37 and accompanying text.

[82]. *See* Pinsky, *supra* note 19, at Part III <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>.

[83]. *See id*.

[84]. *See id*. at Part III.A.3.

[85]. The physical security stems from the mathematical improbability that the document was not signed by the signer. *See* discussion *supra* notes 40-45 and accompanying text. *See also* KOOPS, *supra* note 6, at 37-38.

[86]. *See* SMEDINGHOFF, *supra*, note 40, at 50.

[87]. *See id*.

[88]. *See id*.

[89]. *See Digital Signature Guidelines*, *supra* note 2, at 50.

[90]. *Id*.

[91]. *See id*. at 90-92.

[92]. *See* Smedinghoff, *supra* note 40, at 51.

[93]. *Id*. (emphasis added).

[94]. *See* Pinsky, *supra* note 19, at Part III.A.4 <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>.

[95]. The ABA's *Digital Signature Guidelines* are "intentionally silent" about a definitive standard of care that a subscriber has to not "divulge" her private key. *See Digital Signature Guidelines*, *supra* note 2, at 80 cmt. 4.3.2. However, comment 4.3.2 notes that the standard of care may be resolved by a statute such as the Utah Digital Signature Act. *See id*. (citing UTAH CODE ANN. Section 46-3-305 (1996) giving alternative standards of care for a sender's private key).

[96]. *See Digital Signature Guidelines*, *supra* note 2, at 90-91.

[97]. *See id*. at 91.

[98]. *See* Bill Morton, *The Beginner's Guide to Pretty Good Privacy, Version 1.1* (visited November 4, 1999) <http://www.stack.nl/~galactus/remailers/bgapgp.txt>.

[99]. *See* SMEDINGHOFF, *supra* note 40, at 57 (noting how a date or time affixed by a computer system can be falsified by simply resetting the system's calendar clock).

[100]. *See* Pinsky, *supra* note 19, at Part III.A.5 <http://www.lsus.edu/classes/csc101/spring98/MAR24/GORYDETL.HTM>.

[101]. *See* SMEDINGHOFF, *supra* note 40, at 57.

[102]. *See id*.

[103]. *See* U.C.C. Section 1-206(1) (1995) (requiring the sale of goods over $500 to be evidenced by "some writing" signed by the defendant).

[104]. *See id*. Furthermore, courts have held that a variety of electronic documents are writings under the statute of frauds: *See, e.g.,* Joseph Denunzio Fruit Co. v. Crane, 70 F. Supp. 117 (S.D. Cal. 1948) (finding telex is a writing); McMillan Ltd v. Weimer Drilling & Eng. Co., 512 So.2d 14 (Ala. 1986) (finding mailgram is a writing); Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212 (D. Colo. 1972) (finding tape recording is a writing); Bazak International Corp. v. Mast Industries, Inc., 73 N.Y.2d 113, 7 U.C.C. Rep. 2d

1380 (1989) (finding faxes assumed without discussion to be writings under UCC 2-201); American Multimedia Inc. v. Dalton Packaging, Inc., 143 Misc. 2d 295, 540 N.Y.S.2d 410 (Sup. Ct. 1989) (finding faxed purchase order assumed to be a writing for purposes of a federal arbitration statute); People v. Avila, 770 P.2d 1330 (Colo. Ct. App. 1988) (finding recording on computer disk was a "writing" for purposes for forgery statute); *see also* Clyburn v. Allstate, 826 F. Supp. 955 (D.S.C. 1993) and People v. Rushton, 254 Ill.App.3d 156, 626 N.E.2d 1378 (2d Dist. 1993) (holding that computer printout was a "written result" for purposes of a blood test result statute (625 ILCS 5/11-501.4), and that the computer memory of the results of the test itself was a writing). *But see* Roos v. Aloi, 127 Misc. 2d 864, 487 N.Y.S.2d 637 (Sup. Ct. 1985) (holding that tape recording is not a writing); and Georgia Dept. of Transportation v. Norris, A96A0800 (Ga. Ct. App. July) (holding that fax is not a writing).

[105]. *See* Pinsky, *supra* note 19.

[106]. *See id*. at Part III.B.1.

[107]. *See id*.

[108]. *But see* UTAH CODE ANN. Section 46-3-301 (1996) (requiring licensed certification authority to use only a trustworthy system to issue, suspend or revoke a certificate; to give notice of issuance, suspension or revocation of system; and to create a private key. Also, licensed certification authority must disclose any certification practice statement, and any fact material to either the reliability of a certificate which it has issued or its ability to perform its services).

[109]. *See* KOOPS, *supra* note 6, at 45.

[110]. *See* Clarendon Trust v. Dwek, 970 F.2d 990, 993-94 (1st Cir. 1992).

[111]. *See id*.

[112]. *See* Adam White Scoville, "*Clear Signatures, Obscure Signs,*" 17 CARDOZO ARTS & ENT. L.J. 345, nn. 44-45.

[113]. *See* Pinsky, *supra* note 19, at Part III.B.1.

[114]. *See* FED. R. EVID. 1001-08.

[115]. FED. R. EVID. 1001(3).

[116]. Hearsay is "a statement, other than one made by the declarant, while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FED. R. EVID. 801(c).

[117]. *See* Scoville *supra* note 112, at n.46.

[118]. *See* FED. R. EVID. 803(6).

[119]. *See* Mark S. Dichter and Michael S. Burkhardt, *Electronic Interaction in the Workplace: Monitoring, Retrieving, and Storing Employee Electronic Communications in the Workplace* (visited Oct. 14, 1999) <http://www.mlb.com/speech1.htm>.

[120]. *See id*.

[121]. *See* FED. R. EVID. 1001(3).

[122]. UTAH CODE ANN. Sections 46-3-101 to 46-3-309 (1995).

[123]. For a detailed list and description see McBride, Baker & Coles, *Summary of Electronic Commerce and Digital Signature Legislation* (visited Sept. 9, 1999) <http://www.mbc.com/ecommerce/ds_sum.html>.

[124]. *See id*. *generally* (describing "Any Electronic Signature" statutes). *Id*.

[125]. *C.f. id*. (regarding attributes usually present in statutes that address "Electronic Signatures with specified authentication attributes only"). *Id*.

[126]. *See id*.

[127]. *See* UTAH CODE ANN. Section 46-3 (1998).

[128]. *See id*. Sections 46-3-301 to 46-3-309.

[129]. *See id*. Sections 46-3-201 to 46-3-204.

[130]. *See id*. Section 46-3-401.

[131]. *See id*. Section 46-3-402.

[132]. *See generally Digital Signature Guidelines*, *supra* note 2, at 82 (asserting that digitally signed messages are as enforceable as ink-signed messages written on paper).

[133]. CAL. CODE REGS. tit. ii, Sections 22000-22005 (1998).

[134]. *Id*. Section 22000.

[135]. *Id*. Section 22001; *see also* California Secretary of State official website, *How do we Choose Between a Public Key Infrastructure (PKI) System and a "Signature Dynamics" System?* (visited Feb. 9, 2000) <http://www.ss.ca.gov/digsig/digsigfaq.htm#choose>.

[136]. *See* CAL. GOV'T CODE Section 16.5 (West 1998); *Compare with* UTAH CODE ANN. Sections 46-3-401, 46-3-304 (digitally signed message is presumed valid by the court and the recipient of the digital signature is presumed not to know that the signer: "(i) breached a duty as a subscriber; or (ii) does not rightfully hold the private key used to affix the digital signature....").

[137]. *See* CAL. CODE REGS. tit. ii, Section 22003.

[138]. *See* CAL. GOV'T CODE Section 16.5 (West 1998).

[139]. For additional information, see McBride, Baker & Coles, *Summary of Electronic Commerce and Digital Signature Legislation* (visited Oct. 7, 1999) <http://www.mbc.com/ecommerce/legis/california.html>.

[140]. *See* VA. CODE ANN. Sections 59.1-467-59.1-469 (Michie 1999).

[141]. *Id*. Section 59.1-467.

[142]. *Id*. Section 59.1-468.

[143]. The ALI and the NCCUSL together created the Uniform Commercial Code. Unfortunately, the ALI has passed UETA without the support of the NCCUSL. And the NCCUSL has passed UCITA without the support of the ALI.

[144]. *See* UCITA Draft Section 107, *available at* The National Conference of Commissioners On Uniform State Laws (visited Feb. 9, 2000) <http://www.law.upenn.edu/bll/ulc/ulc_frame.htm>.

[145]. Although the National Conference of Commissioners on Uniform State Laws (NCCUSL) passed UCITA, the model law has significant opposition. *See,* Brenda Sandburg, *E-Commerce Plan Faces Tough Fight*, Cal Law, Aug. 4, 1999, *available at* (visited Feb. 9, 2000) <http://www.callaw.com/stories/edt0804e.html>.

[146]. *See* McBride Baker & Coles, *Summary of Electronic Commerce and Digital Signature Legislation*, <http://www.mbc.com/ecommerce/legis/congress.html> (visited Oct. 14, 1999).

[147]. H.R. 1572, 106th Cong. (1999); *see also* Thomas - U.S. Congress on the Internet (visited Feb. 9, 2000) <http://thomas.loc.gov/>; <http://www.mbc.com/ecommerce/legis/congress.html#1999_House_Bill_1572>.

[148]. H.R. 1714, 106th Cong. (1999); *see also* Thomas - U.S. Congress on the Internet (visited Feb. 9, 2000) <http://thomas.loc.gov/>; <http://www.mbc.com/ecommerce/legis/congress.html#1999_House_Bill_1714>.

[149]. *See* 1999 Bill Tracking H.R. 1714, 1999 Bill Tracking H.R. 1572 <http://thomas.loc.gov/>.

[150]. *See* McBride, Baker & Coles, *Summary of Electronic Commerce and Digital Signature Legislation* (visited Oct. 14, 1999) <http://www.mbc.com/ecommerce/ds_sum.html>.

[151]. The EU employs the term "advanced electronic signature" instead of "digital signature." *See* European Electronic Signature Standardization Initiative ("EESSI"), Final Report of the EESSI Expert Team, July 20, 1999, para. 3.2.1 (defining signature) [hereinafter EESSI Report].

[152]. *See* McBride, Baker & Coles, *Summary of Electronic Commerce and Digital Signature Legislation, European Union* (visited Oct 14, 1999) <http://www.mbc.com/ecommerce/legis/eu.html#EUROPEAN COMMISSION 297>. The Directive became effective twenty days after its presentation to the Council.

[153]. *See id*.*; see also* European Commission, *European Parliament and Council Directive On A Common Framework for Electronic Signatures, Explanatory Memorandum*, at I (visited Oct. 14, 1999) <http://www.ispo.cec.be/eif/policy/com98297.html> [hereinafter *Explanatory Memorandum*].

[154]. *See Explanatory Memorandum*, *supra* note 84, at I.

[155]. *See id*. at I.

[156]. *See id*. at I.

[157]. *See id*. at II.

[158]. *See supra* note 19, at I, II, and III.

[159]. *Id*.

[160]. *See id*. at III.

[161]. *See id*.

[162]. *Id*.

[163]. *See id*.

[164]. *See id*.

[165]. *See id*.

[166]. EESSI Report, *supra* note 151, at Executive Summary 1.

[167]. *Id*.

[168]. *Id*.

[169]. *See id*. at 2.

[170]. UNCITRAL, Model Law on Electronic Commerce with Guide to Enactment (1996) (visited Oct.21, 1999) <http://www.uncitral.org/en-index.htm>.

[171]. The latest Draft Uniform Rules provide two options to the committee: incorporation of the Draft Rules into the Model Law, or a separate "Model Law" exclusively relating to electronic signatures. According to the language of the latest release of the draft (Nov. 23, 1998) the Committee is still considering a separate "Model Law;" *see Draft Uniform Rules on Electronic Signatures*, *Report of the Working Group on Electronic Commerce*, U.N. Commission on International Trade Law (UNCITRAL), 34th Sess., U.N. Doc. A/CN.9/WG.IV (Nov. 23, 1998) *available at* UNCITRAL, *Draft Uniform Rules on Electronic Signatures* (visited Sept. 4, 1999) <http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-79.htm>.

[172]. *See id*. at Part II, Ch. II, Section I, Art.1 (defining "Electronic Signatures" in a way that satisfies article 7(1)(a) of the Model Law).

[173]. Draft Uniform Rules, *supra* note 171.

[174]. *See generally id*. at Introduction, para. 4 (stating that "the Uniform Rules should be consistent with the media-neutral approach taken in the UNCITRAL Model Law on Electronic Commerce. . .").

[175]. *See id*. at Part I, General Remarks, para. 13.

[176]. *See id*.

[177]. *See id*. at Part II, Ch.I, para. 17.

[178]. *See generally id*. at Part I, Ch. III, Art. 13 Attribution of data messages (excepting messages for which the receiver has been notified by the apparent originator that the message did not originate from that person, and the receiver has had "reasonable time to act accordingly;" and, excepting messages in cases where "the addressee knew or should have known," had reasonable care been exercised, that the message was not from the apparent originator). *Id*.

[179]. *See id*. at Part II, Ch. II, Section II, Art. 7.

[180]. *See generally id*. at Part II, Ch. II, Art. 3 (explaining that the presumption of authenticity is invalidated if: 1. "the [originator] [holder] can establish that the [secure electronic signature] [private key] was used without authorization and that the [originator] [holder] could not have avoided such use by exercising reasonable care;" or, 2. "the relying party knew or should have known, had it sought information from the [originator] [certification authority] or otherwise exercised reasonable care, that the [secure electronic] [digital] signature was not that of the [originator] [holder of the private key]"). *Id*.

[181]. *See id*. at Part. II, Ch. II, Section II, Art. 5, para. 35.

[182]. *See generally id*. at Part II, Chapter III, Arts. 11-12 (detailing where Article 11 addresses rights and obligations which are as to the agreement between parties, certificate of authority which may, by agreement, limit liability (but not from intentional recklessness, and where Article 12 addresses liability in the absence of a liability agreement).

[183]. *See supra* note 2.

[184]. *See Digital Signature Guidelines*, *supra* note 2, at 5.

[185]. *See supra* Section II.

**Related Browsing**