THE ABA'S DIGITAL SIGNATURE GUIDELINES: AN IMPERFECT SOLUTION TO DIGITAL SIGNATURES ON THE INTERNET

Edward D. Kania*

During the past ten years, the internet has emerged from an obscure collection of military and scientific databases linked together for national security purposes[1] to the current global system providing access to a multitude of artistic, entertainment and commercial sites. Any individual with access to a computer and an internet account may now participate in a global exchange of knowledge and ideas without having to leave the confines of his home. Consequently, the internet is changing the way that we, as a society, interact, gather information and entertain ourselves.

In addition to access to information, the internet is also changing the manner in which commercial transactions occur. Through the use of webpages,[2] merchants are now able to create virtual storefronts on the internet, allowing them to display images and descriptions of their products, allow for interaction between the consumer and the commercial entity and promote the purchase of the goods. Due to the global nature of the internet, the physical location of the seller is irrelevant to its consumer base that can, regardless of their locale, examine and purchase the business' goods.

The internet also allows individuals to complete business contracts quicker and more efficiently. Through the use of electronic mail ("e-mail"), an individual may instantaneously transmit a contract offer to another party. That party, regardless of location, can then review the document, consent to its contents by accepting the offer and instantaneously re-send the document back to the originating party. This results in more expedited transactions and overall lower transaction costs.

Internet transactions are particularly cost effective for those businesses that are content providers.[3] By advertising and selling their content on the internet, a business eliminates overhead costs such as stores, sales staff and the costs of maintaining adequate levels of inventory. They can pass these savings along to the consumer by means of lower prices.[4] The content providers will also be able to eliminate the problem of the understock-

* Edward D. Kania is an associate with the Washington, D.C. telecommunications law firm of Bennet & Bennet, PLLC where he specializes in cable television, alternative video services and internet matters.

1 One of the principal reasons behind the creation of the internet was to ensure that lines of communication between numerous military and scientific databases would remain intact after a national emergency such as a nuclear strike. *See* Sean Selin, *Governing Cyberspace: The Need for an International Solution*, 32 GONZ. L. REV. 365, 367-68 (1997). Simplified, the internet is a redundant set of connections between various databases. *See id.* By creating this configuration, the military was ensured that even if one link was destroyed, it could continue to transmit information through surviving locations. *See id.* Eventually, non-military uses of the internet developed evolving into the present day internet. *See id.*

2 A webpage is nothing more than an information site which can be purchased by individuals or commercial entities. The webpage acts as a storefront in which the owner may advertise and sell his or her product. One can succinctly define a "webpage," or alternatively a "website," as "a collection of files stored on a file server that is accessible to users of the World Wide Web, a network of servers and information available on the internet." Susan A. Dunn, *Negotiating Web Site Agreements*, 16th ANNUAL INSTITUTE ON COMPUTER LAW, PRACTISING LAW INSTITUTE PATENTS, COPYRIGHTS, TRADEMARKS AND LITERARY PROPERTY COURSE HANDBOOK 467, 469 (1996).

3 Content providers are those businesses that mass produce copies of musical, artistic or literary works. Such providers include record and book stores and their suppliers.

4 An example of this new type of retailer is Amazon.com, which contends it is the world's largest bookstore due to the fact that it claims to hold on its virtual shelves 10 times as many books as even the largest physical bookstore (approximately 2.5 million books). *See* Christopher Anderson, *Survey of Electronic Commerce: A River Runs Through It: Amazon.com Offers a Glimpse of the Future.*, ECONOMIST, May 10, 1997. It does this by keeping only the top selling 400 titles in stock. *See id.* It orders the others books from a nearby distributor. Amazon is price competitive and is able to meet or beat most conventional bookstore even when shipping costs are in-

ing of entertainment products. As no physical product is being transferred to the consumer, the retailer will always have sufficient quantity of the product to meet consumer demand.[5] In addition, through new technologies that link television and the internet,[6] content providers are able to tie-in products to commercial television programming. Consequently, by utilizing internet sales, the entertainment industry can reduce costs and use targeted marketing to sell its product.[7]

However, before this commerce explosion can occur, one must develop a method for verifying the transmission of data through the internet. In particular, it must accomplish the ability to verify the "signature" of the transacting individuals readily and provide reasonable security to the transactions.[8] Although several alternative methods for verifying such signatures exist, the most promising method appears to be through the use of digital signatures in which documents are encrypted using a computer key system.[9] To facilitate the adoption of digital signatures as a means of verifying contractual data, the American Bar Association promulgated its Digital Signature Guidelines in 1996,[10] to be used as a model for state and federal digital signature laws. Several states, including Florida[11] and Utah,[12] have already adopted such laws, and several others, including the District of Columbia, are considering such measures. Although these state initiatives are well-meaning, this desired explosion in the commercial use of the internet cannot occur until a federal digital signature law is adopted.[13] In addition, while the ABA Guidelines may serve as a general foundation for this national law, several key provisions of the ABA Guidelines must be revised to ensure that the legal framework behind a national digital signature law is sufficiently comprehensive.

This essay addresses the need for a federal digital signature law and details the structure that such a law should take. It begins by examining the historical basis for digital signatures in commerce and how the new technology of the internet affects many historical preconceptions of signatures. Next, the essay delves into possible solutions to the problem of signatures on the internet. In addition, it focuses on how "digital signatures" actually work and how the concept of digital signatures is the best solution to the dilemma of on-line signatures.

The essay then focuses on several possible models for a digital signature law, including the American Bar Association's Digital Signature Guidelines[14] and Utah's Digital Signature Law,[15] and why a federal digital signature law is preferable to multiple state laws. Finally, the essay addresses several inherent problems in these models and explores methods to ensure that the contracting parties are sufficiently protected legally without being encumbered by a burdensome signature process.

I. THE HISTORICAL BASIS OF "SIGNATURES"

The ability to authenticate data, including the data's source, is a necessary component of any commercial transaction.[16] Before one can undertake a commercial venture, the involved parties must be able to verify the accuracy of the data that is the basis for the transaction,[17] a fact that is true

cluded. *See id.*

5 The internet purchaser receives an electronically-transmitted copy of the original master of the product. Therefore, the seller will never "sell-out" of a particular product if the master is not damaged or destroyed. *See id.* (describing the ability of Amazon.com to rapidly acquire products from the manufacturers and wholesalers).

6 Cable modems are a new technology that are gaining popularity. *See generally* Rob Fixmer, *Microsoft Combines TV, Computer and the Internet*, N.Y. TIMES, Aug. 18, 1998 (visited March 1, 1999) <http://www.nytimes.com> (describing the increased integration of the internet and television). This technology allows for the transmission of both cable television signals and internet connection through the same wiring. *See id.* Consequently, an individual may be able to watch her favorite show and, through her remote control, then search the internet for tie-in items such as books and T-shirts. *See id.*

7 *See id.*

8 *See* Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, 34 SAN DIEGO L. REV. 1225, 1228-29 (1997).

9 *See id.*

10 DIGITAL SIGNATURE GUIDELINES, 1996 A.B.A. SEC. SCI. & TECH. INFO. SECURITY COMMITTEE 1 [hereinafter GUIDELINES].

11 *See* FLA. STAT. ANN. § 282.72-75 (West Supp. 1998).

12 *See* Utah Digital Signature Act, UTAH CODE ANN. 1953 § 46-3-101 et al. (1995).

13 *See* 143 CONG. REC. H7293-03 (daily ed. Sept. 16, 1997) (statement of Rep. Gordon).

14 *See* GUIDELINES, *supra* note 10.

15 *See* Utah Digital Signature Act, *supra* note 12.

16 *See* David R. Warner, Jr., *Authenticating Digital Signatures*, NETWORK2D NEWSLETTER (ABA Sec. Law Management Practice, Chicago, Ill.), Winter 1996, (visited Mar. 1, 1998) <http://www.abanet.org> [hereinafter Warner].

17 *See id.*

for even the most basic cash transactions.[18] This verification is normally accomplished by confirming the data's source and the identity of the contracting parties.[19] In this way, the parties are held liable for the accuracy of the data, including any promises either explicitly or implicitly transmitted within that data.[20]

Traditionally, contracting parties have used certain formalisms, such as signatures and seals, as a means for verifying the identity of the parties.[21] When used within a contract, these formalisms will legally bind the parties to the transmitted data and will legally verify the author's identity.[22] Therefore, use of these formalisms within a contractual situation has been seen as necessary for the orderly flow of commerce.

The signature is the most commonly used formalism in modern written commercial transactions.[23] While certain types of contractual relationships, such as those lasting more than one year, are voidable unless signed by the parties;[24] other contracts, while not per se invalid, are unenforceable in court if not signed.[25] Consequently, a signature not only verifies the party's identity in a transaction but also, in certain circumstances, is a mandated element of a legally enforceable contract between the signatories.

Webster's Dictionary defines the term "signature" as "the name of one as written by oneself."[26] However, as used in the legal context, the definition is much broader. According to Uniform Commercial Code 1-201(39), "signed includes any symbol . . . executed or adopted by [a] party with present intention to authenticate [a] writing."[27] Therefore, one need not limit a "signature" to the cursive writing of an individual's name. Rather, a signature may include a mark or symbol, as long as that symbol is used with the party's present intent to authenticate a writing.

However, not all signatures will be sufficient to evoke the legal protections given to signed documents. For one to consider a signature legally acceptable, it must demonstrate the attributes of both signer authentication and document authentication.[28] "Signer authentication" refers to whether the signature is sufficiently explicit to denote who has signed the written document.[29] In addition, the signature must be sufficiently unique so another individual may not reproduce the signature without authorization.[30] Likewise, if the signature is so generic that it cannot be verified, it is useless in binding the signatory to the signed document.

One means to overcoming these hurdles is the use of a notarizing system in which a neutral third party, the "notary," authenticates the validity of the signature after the party has sufficiently proven his identity to the notary.[31] Commonly, a notary verifies the signature by reviewing the signatory's personal identification such as a passport or drivers license. The notary affirms the signatory's identification through a notary stamp and a contracting party may legally rely on the notary's verification that the signature is authentic.[32]

"Document authentication" requires that the signature identify the data the signatory accepted so one may not alter the data after the signature has occurred.[33] The parties accomplish this by requiring the signature on the embodiment of the data so that no one can alter the document after the parties sign it.[34] In this way, both parties are assured that the data to which they attested by signing the document is the same data that is transmitted to the other party.

---

18 A purchasing party must feel confident that the representations made about the sold item are correct (*i.e.*, that a purchased sweater is 100% wool or a new type of knife will never need sharpening). Similarly, the selling party must be assured that the data contained in the transferred currency is correct (*i.e.*, that the piece of paper given to the seller actually represents a certain monetary amount).

19 *See id.*

20 Judge Learned Hand stated "[a] man must indeed read what he signs, and he is charged if he does not . . ." Gaunt v. John Hancock Mut. Life Ins. Co., 160 F.2d 599, 602 (2nd Cir. 1947).

21 *See id. See also* Lon L. Fuller, Consideration and Form, 41 COLUM. L. REV. 799, 800 (1941).

22 *See id.*

23 *See* Warner, *supra* note 16.

24 *See* U.C.C. § 3-401 (1990).

25 *See* GUIDELINES, *supra* note 10, at 5.

26 WEBSTER'S II NEW RIVERSIDE UNIVERSITY DICTIONARY 1083 (1988).

27 U.C.C. § 1-201(39) (1998).

28 *See* GUIDELINES, *supra* note 10, at 6.

29 *See id.* at 7.

30 *See id.*

31 *See id.* at 16, 37-38. (discussing the role of a "CyberNotary").

32 *See id.* at 38.

33 *See id.* at 8.

34 The involved data is usually placed in a standard written form with the signature placed below the data. *See* GUIDELINES, *supra* note 10, at 8. Alterations to the data can then be determined by relying on the physical dimensions of the paper used, any obvious changes to the document (*i.e.* whiteout) and the layout of the text. *See id.*

II. THE NEED FOR "SIGNATURES" ON THE INTERNET

Because signatures are a vital element of commerce, consumers must develop the ability to sign documents transmitted over the internet. The nature of the internet, where all communications are typed rather than handwritten, does not lend itself to traditional notions of "signatures." It is not sufficient on the internet to use the traditional method of fixing one's signature at the end of a document since such a method cannot meet the dual authentication requirements. First, the signature will not meet the signer authentication requirement, as the signature will possess no unique characteristic that will ensure the identity of the signatory.[35] Since all communications on the internet are typewritten, there is no opportunity to evaluate the uniqueness of a signature to determine if it is authentic. In addition, traditional notions of a notary reviewing the signed document are impractical since the notary is in no better position to authenticate the signature than the contracting parties.

Likewise, document authentication is more difficult to accomplish on the internet. As previously discussed, the validity of the data contained in "paper" transactions is much easier to ascertain by examining the document for any obvious alterations. However, digital documents are relatively easy to reproduce and alter, and such modifications are nearly impossible to detect.[36] In addition, it is almost impossible to determine whether the document was altered before or after it was signed.

Since internet commerce cannot operate under the traditional notions of signature verification, we must develop a new verification regime for such commerce. Several alternatives currently exist which seek to solve this internet signature problem. One proposed solution is the use of encryption technology to ensure the integrity of the communication. This allows the signatory to "encode" the signed document. Only the receiving party would be able to decode the document using a special code, called a "public key." The use of a public key encryption scheme enables the recipient of an encrypted message to verify the integrity of the message and ensure that no alteration has taken place, thereby satisfying the document authentication requirement for "signatures."[37] However, as this system uses "public keys" available to a wide range of people rather than any type of "private keys" used only by one person, there is no way to verify the identity of the signatory.[38] Therefore, the encryption carries no legal weight to "bind" the encrypting party to the document's underlying facts and will not satisfy the signer authentication prong.

A second possible solution is the concept of "digital" signatures,[39] which are based on the creation of an asymmetric cryptosystem. An individual seeking to use such a system would be required to develop two cryptography keys which would be distinct for that individual.[40] The "keys" are actually two different but related mathematical algorithms that one develops by use of an appropriate computer system.[41] The individual encrypts their message by using the first "private" key, known only to the individual. At that point, the recipient receives the message in the encrypted form.

The recipient receives the location of the second, "public" key to decode the message. A neutral third party holds and surrenders this "public" key to the recipient upon request. The recipient then uses the "public" key to decode the message so he could read it.[42]

An underlying technological process, termed

---

35 *See* Emilio Jaksetic, *How to Ensure the Integrity of Digitally Transmitted Documents*, CORP. LEGAL TIMES, Aug. 1996, at 21.

36 *See id.* (discussing the threats posed to the authenticity and integrity of digital documents).

37 Under the public key encryption scheme, one cannot unscramble a message unless the proper public key is used and no alternation in the document has occurred. *See id.* Therefore, if the recipient receives and successfully unscrambles the message, he may be confident that one has not altered the message. *See id.*

38 *See* GUIDELINES, *supra* note 10, at 46.

39 The term "digital signature" has grown to include a host of different technologies as well as the general concept of affixing personal responsibility for the transmission of data in "cyberspace." *Id.* at 32-33. For purposes of this paper, the term "digital signature" will be used to refer to the creation of an asymmetric cryptosystem for verifying the identity of the signatory and ensuring the integrity of the signed record. *See id.*

40 *See* Charles R. Merrill, *Proof of Who, What and When in Electronic Commerce Under the Digital Signature Guidelines*, 525 PRACTISING L. INST. PAT. 131, 133-34 (1998).

41 *See* Henry R. King, Note, *Big Brother, The Holding Company: A Review of Key-Escrow Encryption Technology*, 21 RUTGERS COMPUTER & TECH. L.J. 224, 231 (1995).

42 For an in-depth explanation of how digital signature technology operates, *See* GUIDELINES, *supra* note 10, at 3.

the "hash function," is the secret to the success of the "digital signature." A "hash function" is an algorithm which produces a unique digital representation, or "fingerprint," called a "hash result" which is imbedded in the text of the signed document.[43] The hash result is based on the use of the "private key" and the specific message to be signed. It is impossible for any two "hash results" to be identical since any change in either the private key or in the text of the message results in a different "hash result."[44] The nature of the "hash function" makes it unfeasible to either derive the original message from knowledge of only the hash result or to alter the content of the message without changing the hash result.[45]

The recipient's use of the "public key" reverses the process of creating this "hash result." By using the public key and the hash result contained in a received message, the recipient "recreates" the original message. However, if the message was originally forged (a private key which does not correspond to the public key was used to sign the message), the public key will not properly interact with the hash result and the recipient cannot retrieve the message. Likewise, if one alters the message prior to its receipt, then it will alter the hash result and one cannot recreate the original message from the public key.

The "digital signature" system accomplishes the necessary authentication requirements for a legally-binding signature.[46] For the system to work one must use corresponding private and public keys in order to allow the recipient to ascertain the identity of the signatory.[47] Since only the signatory has possession of the private key, only that person will be able to "digitally sign" a document so that it may be unencrypted by the recipient. Therefore, one would meet the signer authentication requirement. Similarly, since message alteration would be readily apparent because the public key will not successfully interact with the message's hash result, the integrity of the document would be readily ascertainable. One can ensure the confidence of the recipient that no alteration has taken place during the transmission of the message by enabling the recipient to retrieve the encrypted text. Consequently, one would meet the requirement of document authentication.[48] Digital signatures would therefore appear to be the means by which internet commerce could achieve the "signature" requirement necessary for commercial transactions. The creation of a uniform system for implementing this new technology would allow for the quick integration of new users into the system and would create the entities necessary for the overall operation of the digital signature system.

In 1996, the Information Security Committee of the American Bar Association promulgated Digital Signature Guidelines to try to meet this need for a method of authenticating signatures on the internet.[49] While the Guidelines do offer a technical and legal structure for a digital signature system, they are not intended to serve, in their current form, as a model for a digital signature statute.[50] Rather, the Guidelines serve only as the starting point for the design of a "reliable" system and an appropriate digital signature statute.

It is critical, at this juncture, to realize the dual role that the Guidelines seek to play in the creation of a reliable signature authentication system.[51] Because several alternative means of verifying document and signature integrity exist, such as public key encryption, the Guidelines must not only devise a legal strategy for regulating the best signature authentication system, it must advocate

43 GUIDELINES, *supra* note 10, at 10. *See also* Randy V. Sabett, *International Harmonization in Electronic Commerce and Electronic Data Interchange: A Proposed First Step Toward Signing on the Digital Dotted Line*, 46 AM. U.L. REV. 501, 522-23 (1996).

44 *See* GUIDELINES, *supra* note 10, at 10-11.

45 *See* C. Bradford Biddle, Comment, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L. REV. 1143 (1996).

46 *See* Gary W. Fresen, *What Lawyers Should Know about Digital Signatures*, 85 ILL. B.J. 170 (1997).

47 *See* Anthony Martin Singer, Note, *Electronic Commerce: Digital Signatures and the Role of the Kansas Digital Signatures Act*, 37 WASHBURN L. J. 725, 731 (1998).

48 *See* Scott N. Godes, Note, *Government Contracting on the Internet: Abandoning FACNET as the Government's Network for Electronic Commerce*, 26 PUB. L. J. 663 (1997).

49 *See* William E. Wyrough, Jr. & Ron Klein, *The Electronic Signature Act of 1996: Breaking Down Barriers to Widespread Electronic Commerce in Florida*, 24 FLA. ST. U.L. REV. 407, 432 (1997).

50 *See* GUIDELINES, *supra* note 10, at 20.

51 Although the Guidelines serve this dual role of system creation and system regulation, this essay will only address the latter role. Obviously, if regulators adopt another means for verifying signatures on the internet (*i.e.*, encryption), the Guidelines would be useless in regulating such a system. Therefore, this essay will assume that an asymmetric cryptography system is the most desirable means of verifying such signatures. Consequently, the sole question to be addressed in this paper is how to best regulate this asymmetric cryptography system.

a particular authentication system.[52] In meeting this hurdle, the Guidelines argue for the implementation of an asymmetric cryptography system to verify internet signatures. In addition, the Guidelines create three separate yet interconnected entities that will interact in every digital signature transaction. Based on that proposed system, the Guidelines then turn to the task of assigning legal rights and duties to the systems participants.

III. THE PROPOSED ASYMMETRIC CRYPTOGRAPHY SYSTEM

The Guidelines envision three distinct entities participating in the digital signature system: the subscriber, the certification authority, and the recipient. To begin the signatory process, the subscriber, who is the prospective signatory, must create a public and private key pair, using an appropriate computer program which has been identified as a "trustworthy"[53] method.[54] Since the key pair is reusable, the subscriber may perform an unlimited number of signatures using the same key pair. Once the subscriber generates the key pair, he then delivers a copy of the public key, as well as proof of the subscriber's identity, to the certification authority. The subscriber, however, will retain his private key and will not disclose it to anyone, including the certification authority.

The certification authority serves as an intermediary between the subscriber and the recipient. It is the authority's responsibility to confirm both the subscriber's identity and the validity of the subscriber's key pair.[55] In this manner, the certification authority serves a function similar to a notary: to act as an impartial verifying agent for the subscriber's signature.

Once the certification authority has verified the subscriber's identity and that the private and public keys are a functioning key pair, it issues a "certificate." The certificate lists the subscriber's name, other identifying information about the subscriber, and the subscriber's public key.[56] The certification authority then presents the certificate to the subscriber who "accepts" the certificate by verifying the accuracy of the contained information.[57] Once the subscriber "accepts" the certificate, he may then begin to use the key pair to "digitally sign" documents.[58]

The guidelines require the certification authority to place all of its current certificates in an online repository for access by potential recipients.[59] In addition, the certificate authority must also place, in the repository, a certification practice statement.[60] This document explains the general methods employed by the certification authority to verify subscribers. In addition, the statement includes reference to some other reliable source which will verify the authenticity of the certification authority itself.[61]

The recipient, upon receipt of the encrypted document, would access the repository and the subscriber's certificate.[62] If no valid certificate exists for the subscriber, the recipient would then be placed on notice that the integrity of the digital signature may be in doubt and the signature may be a forgery.[63] However, if a valid certificate exists in the repository, the recipient would use the public key listed in the certificate to retrieve the

---

52 *See* Jane Kaufman Winn, *Open Systems, Free Markets and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1240-41 (1998).

53 The Guidelines define a trustworthy system as:

> [c]omputer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonably reliable level of availability, reliability and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security principles.

GUIDELINES, *supra* note 10, at 54.

54 *See id.* at 78.

55 *See id.* at 68. Since the subscriber retains her private key, the certification authority must devise some means to verify that the subscriber's private and public keys are a functioning key pair. The Guidelines fail to address how this may be accomplished. One solution to this dilemma would be to require the subscriber to use the key pair generation service of a third party which could certify that the keys are a functioning pair.

56 *See* GUIDELINES, *supra* note 10, at 68-69.

57 *See id.* at 21-22.

58 *See id.* at 35-36.

59 *See id.* at 47.

60 *See id.* at 67. *See also id.* at 39-40 (defining a certification practice statement).

61 For the recipient to place any value on the subscriber's certificate, the recipient must first determine the legitimacy of the certification authority. *See* GUIDELINES, *supra* note 10, at 37-38. Since the certification authority's representations regarding the subscriber are key to the viability of the digital signature system, the recipient must be confident that the certification authority is a legitimate entity. *See id.* While the Guidelines do not require that the certification authority be state licensed, the authority, at the least, should use some neutral third party to verify its digital signature. *See id.* The Guidelines envision a long chain of authorities verifying other authorities who verify other authorities. *See id.*

62 *See id.* at 86-89.

63 *See id.*

signed message.[64]

IV. LEGAL RESPONSIBILITIES UNDER THE GUIDELINES

Pursuant to the Guidelines, each of the three entities bears certain responsibilities to ensure the integrity of the digital signature system. If an entity fulfills its obligations under the Guidelines, it will be legally shielded from the consequences of any forged documents. Conversely, an entity which fails to meet its responsibilities may be held liable for the damage caused by a forged document even if the forgery was caused by some third party source. Through this "carrot and stick" approach, the Guidelines seek to create a digital signature system which will ensure the integrity of digitally signed documents.

Pursuant to Guidelines, the subscriber has three distinct responsibilities within the digital signature system.[65] First, the subscriber must provide, upon application for a certificate, truthful data to the certification authority regarding his identity.[66] The subscriber is not entitled to rely, as a defense to misrepresentation of personal data to the authority, on the authority's' failure to independently verify the accuracy of that data.[67]

The subscriber is also prohibited from digitally signing any documents unless a valid certificate exists at the time of the signature or unless the subscriber notifies the recipient that no valid certificate exists.[68] Since the certificate provides verification of the subscriber's identity, the recipient has no independent means of verifying the subscriber's identity absent a valid certificate. Unless the recipient is aware that no certificate exists and that the recipient would be accepting any digitally signed document at his own risk, the subscriber retains full responsibility for all documents which he digitally signs.[69]

Finally, the subscriber must safeguard his private key and, upon knowledge of theft of the private key, must inform the certification authority of the endangerment of the key.[70] A chief tenet of the digital signature system is that only the subscriber or his authorized agent may use the subscriber's private key. If the key is compromised (*i.e.* stolen or copied), it would enable a forger to digitally sign documents in the name of the subscriber without either the certification authority or the recipient being able to detect the forgery. Therefore, the subscriber must ensure the integrity of the private key and must inform the authority of any compromising of the key so that one can suspend the certificate.[71]

While the certification authority has numerous responsibilities under the Guidelines,[72] two of its responsibilities relate to the integrity of the signature system. The authority is responsible for the validity of all statements made within an accepted certificate. This includes warranting that, at the time of the creation of the certificate, the personal information regarding the subscriber is accurate, unless otherwise specifically stated in the certificate, and that the subscriber holds a functioning key pair which has not been compromised.[73] In addition, the authority warrants that it is in compliance with all applicable requirements of the Guidelines.[74] Obviously, to allow recipients to rely on the validity of the certificate, the certification authority must verify that the information contained in the certificate is accurate unless otherwise stated.

It is the responsibility of the authority to suspend or revoke the certificate if necessary. The authority must either suspend or revoke the certificate either upon the request of the subscriber or upon knowledge that representations contained within the certificate are no longer valid or the subscriber's key pair has been compromised.[75] If suspension or revocation is not based on the owner's request, the authority must also promptly notify the subscriber that the certificate is no longer valid.[76] Finally, in all cases, the authority must notify—usually by placing some notice on the certificate itself—all potential recipients seek-

---

64 *See id.* at 117.
65 *See id.* at 101-05.
66 *See id.* at 101-03.
67 *See id.* at 76-77.
68 *See id.*
69 *See id.* at 74-77.
70 *See id.* at 103-06.
71 *See id.* at 77-79.
72 While the Guidelines also require the authorities to have adequate financial resources to operate and require certain record-keeping procedures, these requirements usually apply to the payment of damages for any liability incurred by the authority. *See* GUIDELINES, *supra* note 10, at 63. That is, they do not apply to the integrity of the system. *See id.* Therefore, they are excluded from further discussion in this paper.
73 *See* GUIDELINES, *supra* note 10, at 66-67.
74 *See id.* at 66.
75 *See id.* at 73-74.
76 *See id.* at 74.

ing to verify the subscriber's signature that reliance on the certificate is no longer warranted.[77]

The recipient is charged with one main responsibility to the signature system. A recipient's reliance on a digitally signed document must be "reasonable" even if a valid certificate exists and the public key properly corresponds to the subscriber's private key.[78] For a recipient to "reasonably" rely on a signature, the recipient must have no actual knowledge that either the subscriber or the certification authority has breached any of their various assigned duties under the Guidelines.[79] The recipient must therefore "reasonably" believe both that the certificate is authentic and that the subscriber has not misrepresented any information contained in the certificate or allowed the key pair to be compromised.

In addition to actual knowledge of a breach of the system's integrity, the recipient must also weigh several other factors in determining the "reasonableness" of relying on the signature. These factors include prior dealings between the subscriber and the recipient, the value and importance of the signed message, and usage of trade or any other extrinsic evidence as to the validity of the signature.[80] According to the Guidelines, one must consider these additional factors above and beyond reliance on the certificate.[81] Consequently, the recipient must consider all relevant factors in deciding whether to rely on the digital signature which has been received. Unless these factors indicate that the signature is not reliable, the recipient is legally entitled to rely on the digital signature and the signed message will be deemed to be as "valid, effective, and enforceable as if the message had been written on paper."[82]

The Guidelines are only one possible scheme for regulating digital signatures. However, the industry sources generally approve the Guidelines and they have been used as a basis for the Utah Digital Signature Law,[83] one of the most comprehensive laws on digital signatures in the United States. Because of the Guidelines general acceptance and the overall soundness of its regulatory scheme, it is a proper starting point for a digital signature law. However, several problem areas within the Guidelines, which are detailed below, need to be addressed.

The first important question is which legislative forum should adopt the digital signature laws. As previously stated, several states have already adopted digital signature laws in varying forms.[84] The House of Representatives has considered a federal digital signature law and, on November 8, 1997, the House introduced the "Electronic Financial Services Efficiency Act of 1997," an extremely basic digital signature bill.[85] In addition, there is a strong push occurring among members of the Transatlantic Business Dialogue, held in Rome in November, 1997, for the creation of an international regime for digital signature laws.[86] With legislative action on so many levels containing varying provisions, it is important to determine the most effective legislative level for a new digital signature law while promoting the greatest use of the internet.

A digital signature law enacted at the Federal level would achieve the goals of usability and promote the greatest increase in internet commerce. Because the internet does not lend itself to traditional notions of territorial jurisdiction, the adoption of individual states digital signature laws would thwart the purposes behind digital signatures.[87] Traditionally, the location of the con-

---

77 *See id.* at 75.

78 *See id.* at 86.

79 *See id.* at 87-88.

80 *See id.*

81 *See id.*

82 *Id.* at 106.

83 UTAH CODE ANN. §§ 46-3-101 – 46-3-504 (Michie Supp. 1998).

84 *See* FLA. STAT. ANN. §§ 282.70 – 282.75 (West Supp. 1999); MINN. STAT. ANN. §§ 325K.001 – 325K.27 (West Supp. 1999); UTAH CODE ANN. §§ 46-3-101 – 46-3-504 (Michie Supp. 1998); WASH. REV. CODE ANN. §§ 19.34.010 – 19.34.903 (West Supp. 1999); *See also* Scott Jensen, *AB 811 Regulates the Use of Digital Signatures in Wisconsin*, 71 WIS. L. REV. 23 (1998); Anthony Martin Singer, Note, *Electronic Commerce: Digital Signatures and the Role of the Kansas Digital Signatures Act*, 37 WASHBURN L. J. 725 (1998) [hereinafter Singer]; *Utah Becomes First State to Provide for Digital Signatures*, 15 COMPUTER LAW. 26 (1998). By the spring of 1998, sixteen states had enacted digital signature laws, and eighteen states had digital signature bills pending before their legislatures. *See Singer, supra* at 731.

85 H. R. 2937, 105th Cong. (1997).

86 *See TABD Participants Focus on Electronic Commerce*, EUROWATCH, Nov. 28, 1997.

87 *See* Juan Andres Avellan, *John Hancock in Borderless Cyberspace: The Cross-Jurisdictional Validity of Electronic Signatures and Certificates in Recent Legislative Texts*, 38 JURIMETRICS J. 301, 302 (1998); *see* generally Christopher E. Friel, *Downloading a Defendant: Is Categorizing Internet Contacts a Departure From the Minimum Contacts Test*, 4 ROGER WM. U. L. REV. 293 (1998) [hereinafter Friel]; Katherine Sheehan, *Predicting the Future: Personal Jurisdiction for the Twenty-First Century*, 66 U. CIN. L. REV. 385 (1998) [hereinafter Sheehan]; Michael E. Solimine,

tracting parties determines the law governing the contract.[88] However, due to the ethereal nature of the internet, such notions are unworkable. The internet consists of thousands of separate databases, all located in different jurisdictions, which contain all of the internet's data.[89] For example, a British user, using his laptop computer on a business trip in Florida, could conceivably enter into a contract, over the internet, with an Ohio firm, whose website is located on a Minnesota computer.[90] Determining the law to apply in this transaction would be complex. Therefore, adopting numerous inconsistent state digital signature laws adds another layer of complexity in determining which law to use and would frustrate internet commerce.

It would likewise be problematic to rely on an international regime for digital signatures. Currently, the United States prohibits the exportation of strong encryption software for fear that terrorists and hostile foreign powers will use such technology for improper uses against the United States.[91] Any international agreement would then have to revolve around the use of weaker, less effective encryption software. A digital signature regime cannot properly work without the use of strong encryption schemes to create the key pairs. An international standard would force the United States to either require the use of weaker encryption schemes, which are not currently banned, or to create a dual tier encryption system where contracts created within the United States would utilize one encryption method and contracts created outside the United States would utilize a second type of encryption. In either instance, an international regime would produce an inferior digital signature system with less user protection.

Because state or international law would not assist in the creation of a unified, workable digital signature system, the use of federal law is the only alternative. Federal law would enact one unified digital signature statutory scheme in which the location of the parties and their databases would be irrelevant. A federal law would standardize the requirements for the certification authorities, registration certificates and the type of encryption, and would afford contracting authorities greater legal protection.

V. PROPOSED STRUCTURE FOR FEDERAL DIGITAL SIGNATURE LAW

The Information Security Committee did not intend the Digital Signature Guidelines to serve as a fully-contained, complete model for digital signature legislation. Rather, the Committee realized that any legislation creating a workable digital signature system would need to address the Guidelines' shortcomings.[92] However, even in those areas which are addressed, the system envisioned by the Guidelines is flawed. While the new federal law may take its structure from the Guidelines, several key areas need improvements.

Successful digital signature law must address: (1) privacy protection, (2) the verification of the subscriber's identity, (3) the successful generation of the key pair and its continued integrity, (4) the level of reliance which the signature recipient may attach to the signed document and (5) the procedures for suspending the subscriber's certificate. Unless the digital signature regime can successfully overcome the problems in each of these five areas, the overall regime will fail and will expose the various parties to unwarranted legal liability.

A. Privacy Protection

An effective digital signature law must ensure the confidentiality of both the contents of the contractual data and the identity of the contracting parties. The system has to ensure that the contents of the transmitted document remain confidential to everyone except the contracting parties. For internet transactions, this breach in confidentiality would likely arise if the transmitted document is intercepted, either intentionally or unintentionally by a third party. In addition, privacy is a significant concern for internet contracts since the interception of the document will be sig-

The Quiet Revolution in Personal Jurisdiction, 73 TUL. L. REV. 1 (1998).

88 *See* 8 Richard A. Lord, Williston's Law of Contracts § 19:4 (4th ed. 1998).

89 *See* Reno v. ACLU, 521 U.S. 844, 884-85 (1997), ACLU v. Reno, 929 F. Supp. 824, 831, 848 (1996).

90 *See Sheehan, supra* note 87, at 411-12, 417-20.

91 *See* Glen T. Oxton, *Digital Signatures: Potential and Pitfalls*, N.Y.L.J., Jul. 21, 1997 at S6 [hereinafter Oxton], Alan N. Sutin, *Roadblocks Stall Electronic Commerce, Legal Obstacles Hinder International Trade in Cyberspace*, N.Y.L.J., Jul. 13, 1998 at S6.

92 *See* GUIDELINES, *supra* note 10, at 20.

nificantly harder to detect in internet commerce than in traditional commercial transactions. In current paper contracts, the theft of the contract will be easy to detect since the physical paper will be missing. If the recipient fails to receive the contract, he will quickly know that it has fallen into unintended third party hands. However, with internet contracts, detecting such theft is significantly harder. A third party may intercept the communication and copy its contents without actually stopping the transmission of the data to its intended parties. Therefore, the parties will not know that a third party has possession of their document.

Similarly, while the contents of the document may not be confidential, the identity of the parties to the contract may be extremely private. For example, in the entertainment arena, a third party's knowledge that an intercepted document is a contract for the sale of a manuscript may not be as important as knowing whether the purchasing party is a major film producer or an unknown film school student.[93] Consequently, an effective digital signature regime must address both content and contracting party privacy issues.

The dual key encryption system devised in the Guidelines overcomes these two hurdles. Even if a third party intercepts the document, that party would be unable to unencrypt the document without access to the public key. Without that public key, which one could not acquire from the certification authority without proper authorization, the document is a useless series of unintelligible characters. In the same vein, the third party would be unable to determine the identity of the signatory. Through the use of anonymous e-mail addresses, the signatory could choose to remain anonymous. The unintended recipient would not be able to decipher the signatory's identity and, once again, unless the third party had access to the public key, it could not decipher the message to determine the exact signatory. Therefore, the Guidelines are sufficient in their current form to meet these privacy hurdles and they will need no additional modifications to protect privacy.

B. Personal Information Verification

The Guidelines are insufficient in the area of personal information verification and must be revised for any federal digital signature law. The verification of the personal information of the subscriber is perhaps the most critical element of any digital signature system. The certification authority is charged under the Guidelines with verifying the personal information of the subscriber. The recipient will rely in large part on the certification authority's review of the subscriber's identity and the verification of the subscriber's credentials. If the authority fails to adequately verify the subscriber's identity, an imposter could impersonate a signatory, secure a key pair and begin executing contracts using this false identity. The recipient would be unaware of such fraud until after he had relied on the contract and sought performance of its terms. The Guidelines fail to properly address the problem of adequate verification of the subscriber's personal information throughout the operational period of the certificate. Because the integrity of the digital signature system is largely based on the truthfulness of the representations made by the certification authority in the certificate, the authority must adopt sufficient methods to confirm the subscriber's identity and the integrity of the subscriber's key pair. The Guidelines requires the authority to verify the subscriber's personal information prior to issuing a certificate.[94] while the Guidelines do not suggest a specific method for verifying the data, the Guidelines do require that the authority confirm the information through "appropriate inquiry and investigation."[95] The Guidelines urge the authority to specify, in the certification practice statement, the means by which the certifying authority confirms the information.[96] Therefore, the Guidelines do require a pre-certification investigation but are silent on the exact process for such an investigation.

To allow a certain degree of flexibility, the federal law should create several alternative methods for identity verification which are reliable but not

93 *See* Federal Trade Commission Report to Congress, *Individual Reference Services*, (1997) (visited Feb. 3, 1999) <http://www.ftc.gov/privacy> (containing information concerning online consumer protection). For example, knowledge that a manuscript was being purchased by Steven Spielberg would significantly elevate the status of the manuscript and consequently its price. Therefore, if such knowledge became public, it could begin a bidding frenzy for the manuscript.

94 *See* GUIDELINES, *supra* note 10, at 68.

95 *Id.* at 34.

96 *See id.* at 68.

overly burdensome to the subscriber. Various verification options currently exist, each with their own strengths and weaknesses and each of which could be utilized as a verification method. A certification authority may be able to verify the subscriber's identity through the use of another authority's certification of the subscriber. If the subscriber already possesses a dual key group from another certification authority, that authority would have issued its own certificate regarding the subscriber. The second authority could then simply rely on that certificate for its own verification of the subscriber's identity. Of course, the reliability of the second certificate would only be as good as the verification procedures used in the first certification. In addition, depending on the regulation of certification authorities eventually developed, the first certification authority may falsify a subscriber's certificate if it is a "bad actor" authority.

An alternative verification method is to require in-person verification of the subscriber.[97] Much like the current practice of appearing, in person, to a notary with appropriate personal documentation, the certification authority could require that the subscriber appear at its offices before it will issue a certificate. While this would cut down on the incidents of fraud, it defeats the purpose behind on-line contracts. The basic premise behind internet commerce and on-line signatures is to allow the subscriber to conduct business without having to physically travel to a location. Even though this verification process would only occur one time, some internet purists may feel that the purposes behind on-line contracts are thwarted by even this one-time inconvenience.[98]

Another potential pitfall for subscriber identification is the need to continually update the truthfulness of the subscriber's personal information. In addition to the original verification of the subscriber's identity, the certification authority must also re-verify the subscriber's personal information over the operational life of the certificate. During the term of the certificate, a subscriber's name and address may change, thereby affecting jurisdictional concerns. In addition, the agency relationship contained in the certificate may cease during the operational period. A certificate is useless if it is factually correct at the time of its issuance but later contains outdated, false information. For an effective digital signature system, a recipient must be able to rely on the certificate's validity at all points in the certificate's life.[99] This necessitates re-verification of the subscriber's information during the certificate's life, usually through means similar to those used to initially verify the subscriber.

A re-verification requirement is absent from the current Guidelines. While the Guidelines require an initial verification, there is no continuing duty to re-verify.[100] In fact, in its October 5, 1995 Draft, the Guidelines' authors admit that no re-verification requirement exists in the Guidelines and that none should be inferred.[101] The Guidelines rely solely on the subscriber to notify the certification authority of any factual changes which need to be addressed in the subscriber's certificate.[102]

This "one time" verification of the subscriber's information by the certification authority is a departure from the verification procedures notaries use in "paper" signature transactions.[103] Currently, a signatory must present his identification (usually a driver's license or some other personal identification card) to the notary each time he seeks to have his signature verified. In addition, a notary's notarization applies only to the document to which it is attached and cannot be used to verify the signatory's identity for any other transaction.[104] This is quite different from the Guidelines which require the certification authority to verify the subscriber's identifying information once, even though the certificate could last indefinitely.[105]

---

97 *See Oxton, supra* note 91, at S6.

98 Even in non-internet transactions, some entities are forgoing physical appearance for the purposes of information verification. *See* U.S. State Department—Passport Information Website (visited Feb. 3, 1999) <http://www.travel.state.gov/passporteasy.html>. For example, passport issuance, which at one time required in person verification, may now be done through the mail. *See id.*

99 *See* GUIDELINES, *supra* note 10, at 78.

100 *See id.* at 68.

101 *See* 101 DIGITAL SIGNATURE DRAFT GUIDELINES, at Comment 3.13.2 (American Bar Ass'n Comm. on Info. Sec.) (1995)

102 *See id.*

103 *See* 4 ANDERSON'S MANUAL FOR NOTARIES PUBLIC (1996) (describing the common procedures used by a notary public).

104 *See id.* at 21.

105 The Guidelines do not address the specifics of how the certification authority will verify the subscriber's identity and information. One suggestion made by the Guidelines, however, is that the certification authority rely on any other

The new federal digital signature law must therefore depart from the Guidelines and require regular re-verification of the subscriber's identity. Because the Guidelines shield the certification authority from any liability if an initial verification was conducted, and because the "bad actor" subscriber will have either absconded or will be judgment-proof, it will force the recipient to bear the full brunt of any damages caused by a forged document if it does not mandate re-verification.[106] Placing such a high burden on the recipient, who has fully complied with her responsibilities under the Guidelines, will have a chilling effect on any recipient's willingness to use digital signature technology.

To remedy this omission, the federal law must require re-verification of the subscriber's personal data. The law should require the certification authority, at regular intervals throughout the operational period of the certificate, to re-verify the subscriber's personal data. The method for the re-verification can be the same type implemented for the initial verification and should be specified in the certification practice statement. The authority should also state, in the subscriber's certificate, the date of the last verification. In this way, the recipient may weigh, in addition to the other "reasonableness" requirements of Guideline 5.4, the reliability of a digital signature which he has received based on the length of time since the last certification.

C. Key Generation

The next major hurdle for the federal law to overcome is the issue of the generation of the key pair. Since the feasibility of the system relies on the key pair working properly and inhibiting third party access to the signed documents, federal law must be explicit in how one generates the keys and the computer standards by which one judges the security of the keys.[107]

The Guidelines fail to adequately address the issue of key pair generation by allowing subscribers to generate their own key pair so long as they use a trustworthy system.[108] The limitations of the guidelines encourage fraud and multiple, incompatible generation systems. Therefore, federal law must go beyond the requirements set forth in the Guidelines.

Under the Guidelines, the generation of the key pair is the exclusive responsibility of the subscriber who is required to use a "trustworthy" system.[109] Although the Guidelines do not delineate either a specific cryptographic algorithm or computer system to be used, they do define "trustworthy systems" to be "[c]omputer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonably reliable level of availability, reliability and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security principles."[110] Therefore, any system which appears to meet these requirements would be deemed "trustworthy" under the Guidelines and a subscriber could use the system to generate the key pair.[111]

The Guidelines' position on key generation has several serious flaws. First, by allowing the subscriber to generate his own key pair, the Guidelines allow for the possibility of fraud on the part of the subscriber. If the subscriber is allowed to generate his own keys, the subscriber could generate a key pair system which would allow him to alter digitally signed documents after their transmission (*i.e.* create a key pair which defeats the document integrity ability of the hash results and allows the signatory to alter the document even after it has been signed).[112] Even though a key pair may be "improper," the certification authority may not be able to detect the abnormality and may deem both the key pair and the system used to generate them to be "trustworthy." The ultimate burden of any financial harm caused by a forged document would rest squarely with the recipient since the certification authority would have fulfilled its requirements under the Guidelines and the "bad faith" subscriber would have either absconded or be judgment proof.

Even if the subscriber generates the key pair in "good faith," the lack of a generating system standard may seriously impair the operation of the

digital signature certificate, granted by another certification authority, which the subscriber may possess.

106 *See* GUIDELINES, *supra* note 10, at 88, 104.

107 *See id.* at 52.

108 *See id.* at 78.

109 *See id.*

110 *Id.* at 68.

111 *See id.* at 101.

112 *See* Emilio Jaksetic, *How to Ensure the Integrity of Digitally Transmitted Documents*, CORP. LEGAL TIMES, Aug. 1996, at 21 (providing an explanation of this problem).

signature system. Several digital signature standards currently exist and are in active use.[113] If subscribers are allowed to generate their own key pair, the subscriber may select a generating standard which is incompatible with the certification authority or the digital signature system used by the recipient.[114] Use of multiple key generation standards could lead to the growth of incompatible digital signature systems being developed which would make the use of digital signatures burdensome and unappealing for use in verifying internet contracts.[115]

The federal digital signature law can avoid these pitfalls by creating a fourth entity which would exclusively be charged with generating key pairs. In fact, the Guidelines recognize that, while it does not require subscribers to use a particular entity, key pair generation businesses would likely develop as part of a digital signature regime.[116] This service would be regulated by appropriate law similar to the regulation of the certification authority, and would be operated by a neutral third party whose exclusive task would be to generate key pairs using an appropriate digital signature standard.[117] It would require a subscriber to use such a service to generate his key pairs in conformity with the standard used by his certification authority.[118]

Requiring the use of a key pair generation system would not inhibit the use of digital signatures. The cost of purchasing a key pair from such a service would be a minimal expense[119] which would ensure the interested parties of the integrity of the key pair. Requiring the use of a generation service would eliminate the current problems associated with the Guidelines. The generation of the key pair by a neutral third party would curtail the incidences of fraud because a neutral third party would have no interest in generating an unreliable key pair. Additionally, it would enable the generation authority to certify the manner in which the keys were generated and attest to the integrity of the key pair.[120]

This service would also alleviate some of the problems with the use of multiple digital signature standards. These generation services will advise a subscriber as to the optimal standard to use for his particular needs as well as to the standard's compatibility with the certification authority's system.[121] Therefore, requiring the use of key generation services not only promotes the creation of new business but also shores up the integrity of the digital signature system.

Finally, federal law should establish life spans for all key pairs. As technology continues to advance, older key pairs, while invulnerable at the time of their creation, may become compromised. In addition, the longer the key pairs are in use, the greater likelihood that one may accidentally reveal it to a third party. Requiring the subscriber to regularly re-generate new key pairs will ensure that the pairs are of the highest quality and that they have not been compromised. Since the cost of generating these key pairs is relatively low, this requirement will not impede use of the digital signature system.

---

113 *See id.*; *see also Oxton, supra* note 91, at S16.

114 *Oxton, supra* note 91.

115 An analogous situation may be the dual personal computer systems (*i.e.*, Macintosh compatible vs. IBM compatible) which currently exist. One digital signature system may employ a "X" generation standard while another system may employ "Y." A potential recipient, who possesses the technology to use the "Y" system, would not be able to receive any messages using the "X" technology. Similarly, a subscriber may be forced to have a key pair generated, and certificates verified, for each type of "system" which exists. Both of these scenarios will lead to greater costs for the participants.

116 *See* GUIDELINES, *supra* note 10.

117 One could address the "multiple system" problem by the establishment of a universal key generation standard. *See e.g.*, H.R. 695, 105th Cong. (1998). However, since that question addresses the structure of the digital signature system, and less to its regulation, it will not be further addressed in this essay.

118 The generation service would be required to certify that it has generated the particular key pair which the subscriber has submitted to the certification authority. *See Oxton, supra* note 91, at S15.

119 While this essay does not address the economic feasibility of the Guidelines system, it should be noted that this additional step in using the digital signature system will not be unduly burdensome. Since the Guidelines envision that the subscriber himself would have the technical ability to generate a key pair, such a process cannot be either overly expensive or difficult. Therefore, the per-pair cost of generation of the keys by the generation service should not dissuade individuals from using digital signatures.

120 This certification could be similar to the certification authority's certificate practice statement and be publicly accessible through an on-line repository. *See* Kenneth A. Freeling & Ronald E. Wiggins, *States Develop Rules for Using Digital Signatures, Laws that Govern Transactions using Public Key Cryptography Will Spur Electronic Commerce*, NAT'L L. J., Oct. 20, 1997, at C11 [hereinafter Freeling].

121 *See* Wendy R. Leibowitz, *Laws on E-Sigs Inked, Competing Technologies Test States' Definitions of an Electronic Signature*, NAT'L L. J., Nov. 17, 1997, at A1 (suggesting consumers need protection from fraud when they have little understanding of the system).

D. Digital Signature Reliance by the Recipient

Another major obstacle to a successful digital signature regime is the allocation of risk to the recipient of the signed document. The recipient stands the most to lose from a forged or otherwise improper digitally-signed document and the recipient will bear the brunt of detrimentally relying upon a contract that is later revealed to be invalid or forged. Therefore, before a digital signature system can be widely used in commercial transactions, recipients must be confident that they will receive adequate legal protection under a digital signature law. The drafters must build strong protections into the system so that the recipient may both rely on the signed document and believe that the courts enforce the contract and require the signatory to perform on the contract. Only then will recipients agree to use this media to conduct their business.

The current Guidelines are inadequate to instill confidence in recipients. The Guidelines place a high burden on the recipient and will have a chilling effect on the use of digital signatures. The new federal law must significantly depart from the Guidelines in this area and adequately protect the interests of the recipients.

Under the current Guidelines structure, a recipient is not legally entitled to rely on the signed document simply because a facially valid subscriber certificate exists and the public key, which he obtained from the certification authority, properly unencrypted the signed document. Unlike traditional signatures, where the recipient may rely on the notarization of the signature by a licensed notary,[122] the digital signature recipient must weigh four additional factors before he may reasonably rely on the digitally signed document as genuine.[123] For reliance to be reasonable, the recipient must consider, in addition to the existence of a valid certificate, the following:

> (1) facts which the relying party knows or of which the relying party has notice, including all facts listed in the certificate or incorporated in it by reference,
>
> (2) the value or importance of the digitally signed message, if known,
>
> (3) the course of dealing[s] between the relying person and subscriber and the available indicia of reliability or unreliability apart from the digital signature,
>
> (4) usage of trade, particularly trade conducted by trustworthy systems or other computer-based means.[124]

The Guidelines readily admit that no technology is infallible and, therefore, these factors were introduced to offset technological problems.[125] By adopting these additional factors, the Guidelines seek to shift part of the certification authority's liability for signature verification onto the recipient.

Utah's Digital Signature Act of 1996,[126] which is modeled on the ABA's Guidelines, takes this concept of "conditional reliance" one step further. Under the Utah Act, a certification authority may place, within a subscriber's certificate, recommended monetary reliance limits.[127] A recipient is urged to limit all contracts to the reliance limit because it serves as the maximum damages that one can require the authority to pay for any loss caused by the recipient's reliance on the certificate.

The Guidelines' four reliance factors are an improper attempt to re-allocate risk for these commercial transactions. While the risk of forgery and other improper activity is inherent in digital signatures, it is also inherent in other manners of signature verification. The signing party can equally falsify information to a notary and to a certification authority. Identification can be faked and documents altered in both ink and paper and internet dealings. Therefore, the Guideline's attempts to compensate for deficiencies in the technology of digital signatures are unwarranted.

In addition, the factors cited by the Guidelines would preclude many transactions from occurring via the internet. The Guidelines list the value of the subject matter of the contract, as well as prior dealings between the parties, as two factors to consider when evaluating the validity of the digital signature. This precludes use of this technology

---

122 *See* Michael L. Closen & R. Jason Richards, *Cyberbusiness Needs Supernotaries*, NAT'L L. J., Aug. 25, 1997, at A19. Of course, if a notarized document appears to have been tampered with (*i.e.* apparent erasures, crossed out words, etc.), the recipient may not blindly accept the document as genuine.

123 *See* GUIDELINES, *supra* note 10, at 87. A relying party assumes the risk that a digital signature is invalid if his reliance was "unreasonable." Therefore, this "reasonableness" factor will affect the recipients right to seek damages if the signature is determined to be a forgery. *See* GUIDELINES, *supra* note 10, at 82.

124 GUIDELINES, *supra* note 10, at 87.

125 *See id.* at 88.

126 UTAH CODE ANN. §§ 46-3-101 – 46-3-504 (1996)

127 *See id.* at §46-3-309; *See also Freeling, supra* note 120 at C11.

for larger contracts and for contracts involving first-time contact between the parties. If recipients are only legally protected when their contracts are insignificant or with long-term trading partners, the digital signature system becomes practically worthless for the majority of transactions that could benefit from the use of the internet. The worth of the contract has no bearing whatsoever on the effectiveness of the dual key system or on the verification abilities of the certification authority. Therefore, these factors are not only chilling for the majority of contracts but also have no bearing on the reliability of the signed document.

The Guideline's four factors will have a "chilling" effect on commercial use of digital signatures. Before businesses will adopt the use of digital signatures over traditional signatures, they must be assured that digital signatures are both reliable and are not more burdensome than "ink" signatures. Neither of these conditions is met under the current system. To obtain the same degree of reliance associated with "ink" signatures namely, that the notarized document is authentic absent any glaring tampering, the recipient must weigh past dealings with the subscriber and the "trustworthiness" of the underlying computer systems used. Given the different reliance inquires required by the two signature systems, many businesses will opt to remain with "ink" signatures which require less additional research to verify.

To alleviate this "chilling" effect, the federal law must shift the burden and responsibility of verifying the authenticity of signatures back onto the certification authority. While such a regime would place greater legal liability on the certification authority for any "tainted" signatures, these authorities are in a better position to evaluate the credibility of the subscriber's information and the integrity of the key pairs, the two essential components of the digital signature system. In addition, the certification authorities have the most to gain from a thriving, reliable digital signature system, and more to lose from half-hearted attempts to verify subscribers and their key pairs. The certification authorities have enormous incentive to scrutinize their subscribers and the integrity of the entire digital signature system. Of course, if the recipient has knowledge that a signature is forged or otherwise unreliable, he must be precluded from seeking damages against the certification authority. However, absent that knowledge, the recipient must be able to rely on a received digital signature and the validity of the subscriber's issued certificate.

E. Certificate Suspension/Revocation Procedures

The final issue of concern that the Guidelines fail to properly address is the procedure by which one can suspend or revoke the subscriber's certificate. In traditional ink signatures, the signatory would readily be able to ascertain whether the certification authority (*i.e.* the notary) will authenticate his signature and identity since the notary would either notarize or refuse to notarize the document. However, in the internet, a signatory may properly encode his document using their key pair, only to find out after transmitting the document that the certification authority revoked the subscriber's certification. This would leave the signed document in a legal limbo and adversely impact the subscriber's ability to continue to conduct business. Therefore, the certificate authority must promptly notify the subscriber if his certificate has been suspended or revoked and the certificate authority must assure that revocation and suspension will only occur if "good cause" exists.[128]

Once again, the Guidelines fail in this area. Under the Guidelines, a certification authority may suspend or revoke a certificate in two situations. First, the authority may suspend/revoke a certificate pursuant to a request by the subscriber.[129] This situation will not unfairly affect the subscriber as long as the certification authority has verified that the subscriber, and not an impostor, is seeking the suspension/revocation.

The second suspension/revocation situation is much more problematic. A certification authority may suspend/revoke a certificate, without prior notice or consent of the subscriber, if the authority confirms that a material fact in the certificate is false, a material prerequisite to the issuance of the certificate was not satisfied, or that the integrity of the subscriber's private key has been compro-

[128] *See* Lonnie Elridge, Comment, *Internet Commerce and the Meltdown of Certification Authorities: Is the Washington State Solution a Good Model*, 45 UCLA L. REV. 1805, 1821 (1998).

[129] *See* GUIDELINES, *supra* note 10, at 93.

mised.[130] While pre-suspension/revocation notice is not required, the certification authority must promptly notify the subscriber subsequent to the authority's actions.[131]

The issue of notice to the subscriber involves two divergent, conflicting interests. On the one hand, a recipient must immediately be made aware that the representations made in the certificate may be suspect and that reliance on the signature may not be warranted. Therefore, a certification authority must quickly move to suspend or revoke a suspect certificate before an unwary recipient uses the certificate to rely on a received signature.

In conflict with this genuine concern is the potential damage to the subscriber if his certificate is unfairly suspended or revoked. The revocation of an individual's certificate may seriously disrupt his ability to conduct business.[132] Likewise, the revocation of a certificate implies that the subscriber is either an imposter, a liar or has carelessly lost his private key. These allegations could be devastating to a business's reputation and could seriously impact the subscriber's ability to utilize digital signatures in the future.[133] If the revocation later turns out to be unsubstantiated, the subscriber will have been irrevocably injured without the ability to challenge the suspension/revocation before it became effective.

The Guideline's current policy of not requiring pre-suspension/revocation notice solves the former but not the latter problem. By not requiring pre-revocation/suspension notice, the Guidelines allow the certification authority to quickly suspend/revoke the subscriber's certificate to protect the recipient from harm. While this approach is effective when the underlying reasoning for revocation is later confirmed, it is harmful if the certification authority erred in revoking/suspending the certificate.

The federal digital signature law can overcome this dilemma by creating a new intermediary category placed on the certificate prior to the subscriber's notification. They would place this new designation on the certificate once the authority believes that the integrity of the certificate is in question. However, the certification authority would place the designation on the certificate prior to any notice to the subscriber. The designation would warn recipients that the certification authority is temporarily unable to verify the authenticity of the certificate's underlying facts but that the certificate has been neither suspended nor revoked. It would urge recipients to use additional factors, such as prior contact between the parties and the worth of the signed document, to determine the validity of the received digital signature. It would also notify the recipient that the authority shall be held harmless for any reliance by the recipient on the signature from the time of the designation of the certificate. Finally, the designation would also carry a deadline by which a final decision regarding the certificate would be made by the certification authority.

During the time between the placing of the designation on the certificate and the deadline, the authority would be required to notify the subscriber, who would then have the opportunity to prove the validity of the information contained within the certificate. If the authority is satisfied as to the validity of the certificate, the authority would remove the new designation by the deadline and retroactively "certify" any signature created during the prior questionable period. If the certification authority is unable to verify the subscriber's personal data or the integrity of the key pairs, the authority would formally suspend or revoke the certificate and would retroactively "decertify" all signed documents during the questionable period.

By creating this new designation, the federal law would protect each of the involved parties. The subscriber would be given pre-suspension/revocation notice and an opportunity to prove the validity of the certificate. In addition, if the certificate is found to be factually correct, the subscriber would face minimal business disruption or loss of credibility. The certification authority would be able to notify potential recipients of its concerns regarding the validity of the certified information, but would not be liable for any loss caused by a relying signature recipient. Finally, the recipient would be placed on notice as to potential problems with the certificate and would need to seek additional factors to shore up his reliance on the signature. Therefore, all concerned

130 *See id.* at 73-74.
131 *See id.* at 96-97.
132 *See id.* at 74.
133 Knowledge of prior certificate revocations may impact the "reasonableness" of a recipient's reliance pursuant to Guideline 5.4 "reliance" factors. *Id.* at 87.

parties would be adequately protected under this new designation.

In conjunction with this new category, the new federal law would need to contain a related provision dealing with the recipient's reliance on the signed documents. As previously stated, the recipient is in a somewhat precarious position in the area of reliance. If the recipient receives a document which facially appears to be valid (*i.e.*, the public key works with the document) but no valid certificate exists, the recipient should not rely on the document under the current Guidelines. However, if he fails to accept the contract and, eventually, it is determined that the suspension/revocation was incorrect, the recipient may be liable for breach of contract. Therefore, the federal law must contain a provision stating that the recipient shall not be liable for failing to perform under a contract in which the subscriber's certificate was initially suspended/revoked, but was later reinstated for that time period.

CONCLUSION

While both the internet and digital signatures are still in their infancy, their potential to resculpt the manner in which the public receives information and conducts its business transactions is enormous. Geography and access to transportation become irrelevant as the individual can explore the globe from the comfort of his home. However, like all new technologies, the pace for the public to embrace these new tools is somewhat slow. One must change preconceived notions and patterns before the general public will embrace new technology.

The public must also feel safe in using this new technology. For internet commerce, that entails the knowledge that they will receive the same level of legal protection and security as in traditional ink contracts. While digital signatures appear to be the technological means to promoting and protecting commerce, they are ineffective without a comprehensive digital signature law, preferably at the federal level.

In creating this federal digital signature law, the ABA's Guidelines provide an excellent starting point. However, in several key areas, the Guidelines prove to be counterproductive to the goal of protecting the commercial participants. Through the legal modifications suggested above, a comprehensive, effective digital signature law is within reach. Once a reliable means of ensuring the validity of internet contracts occurs, the paper contract will become the horse and buggy of the new millennium.