Fordham International Law Journal

Volume 22, *Issue* 3 1998 *Article* 11

The Protection and Promotion of E-Commerce: Should there be a Global Regulatory Scheme for Digital Signatures?

Sanu K. Thomas*

*

The Protection and Promotion of E-Commerce: Should there be a Global Regulatory Scheme for Digital Signatures?

Sanu K. Thomas

Abstract

This Note addresses the issue of whether all nations should enact a uniform global legal scheme governing digital signatures for the purpose of promoting E-Commerce. Part I of this Note describes digital signatures and considers their different functions. Part I also discusses E-Commerce and the application of digital signatures to E-Commerce. Further, Part I briefly examines the major legal schemes set up by organizations, states, nations, and international bodies. Part II analyzes arguments for and against global digital signature laws in order to facilitate E-Commerce. Part III argues that nations should adopt a global digital signature legal scheme in order to promote E-Commerce by eliminating conflicting laws. This Note concludes that nations should draft and enact a global digital signature legal scheme.

THE PROTECTION AND PROMOTION OF E-COMMERCE: SHOULD THERE BE A GLOBAL REGULATORY SCHEME FOR DIGITAL SIGNATURES?

*Sanu K. Thomas**

INTRODUCTION

The development of electronic commerce[1] ("E-Commerce") and modern communications technology has created the need and opportunity for new business practices.[2] The growth of E-Commerce affects many sectors of the world economy.[3] By the turn of the twentieth century, one commentator estimates that, in the United States alone, the value of E-Commerce transactions will reach billions of U.S. dollars per year.[4]

---

* J.D. Candidate, 2000, Fordham University School of Law. The author wishes to thank God, his family, Prof. Joel Reidenberg, his colleagues at Credit Suisse First Boston Corporation, the editors and footnoters who have worked on this Note, and all of his friends who have supported him on writing this Note.

1. *See* Holly K. Towle, *Electronic Transactions and Contracting*, 520 PRAC. L. INST.: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 515, 517 (June 8, 1998) (defining electronic commerce ("E-Commerce") as business environment in which advertising, buying and selling and licensing of goods, services, and information occurs electronically). E-Commerce transactions are conduced through networks such as computer networks or wireless communication systems. *Id.* Many types of commercial activities can be facilitated using E-Commerce, such as the transfer of funds, ordering of supplies, and ordering and digital delivery of information or entertainment products. *Id.* E-Commerce offers unique commercial opportunities because of the way in which information relating to goods and services flows. *Id.* The convergence of the computer and telecommunications sectors of our economy has broadened the capacity for digital communication and electronic interaction using cellular phones, hand held computers, high speed wire, cable, and satellite transmissions. *Id.*

2. *See* Stephen S. Wu, *Incorporation by Reference and Public Key Infrastructures: Moving the Law Beyond the Paper-Based World*, 38 JURIMETRICS J. 317, 317 (1998) (stating that E-Commerce will affect how parties enter into contracts); *see also* Towle, *supra* note 1, at 517 (demonstrating that E-Commerce is quickly enhancing or replacing other traditional commercial activities). For example, on January 28, 1998, Egghead, Inc. announced that it would close each of its 80 retail outlets to operate exclusively on the Internet. Towle, *supra*, at 517.

3. Daniel J. Greenwood & Ray A. Campbell, *Electronic Commerce Legislation: From Written on Paper and Signed in Ink to Electronic Records and Online Authentication*, 53 BUS. LAW. 307, 308 (1997); *see* Andrew Urbaczewski et al., *A Manager's Primer in Electronic Commerce*, BUS. HORIZONS 5 (Sept. 1, 1998) (stating that E-Commerce has affected way individuals and organizations purchase goods and services). Projected E-Commerce sales are at US$ 4.8 billion, which doubles 1997 totals. Urbaczewski et al., *supra*.

4. *See* Catherine Lee Wilson, *Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond*, 30 CREIGHTON L. REV. 671 (1997) (estimating that more than

The growth of E-Commerce has raised new issues for businesses conducting transactions on the Internet,[5] one of which is how they will enter into contracts in a manner appropriate for this new electronic[6] environment.[7] The possibility of concluding contracts and other legally significant transactions electronically raises a number of legal and technical questions about how to ensure the authenticity[8] of electronic documents.[9] Scholars have given a great deal of attention to the legal effect of E-Commerce transactions.[10] E-Commerce transactions may not satisfy

---

200 million people will regularly use Internet by 2000); *see also* Diane Francis, *Welcome to the World's Biggest Catalogue Store: Internet Bandwagon Takes You to the Hottest Game in Town*, NAT'L POST, Feb. 9, 1999, at C3 (stating that business conducted on Internet is currently at US$200 billion).

5. *See Reno v. ACLU*, 117 S. Ct. 2329, 2334 (1997) (defining Internet as global network of interconnected computers); *see also* Craig Peyton Gaumer, *Conflicts, The Constitution, and the Internet*, 86 ILL. B.J. 502, 503 (1998) (describing history and original purpose of Internet, which began in 1969 as U.S. Department of Defense project designed to facilitate exchange of information among educational institutions, government agencies, and scientific community). The Internet was designed to make international communication easier because it is a network of decentralized, self-maintaining series of redundant links between computers with the automatic ability to re-route communications if one or more links are damaged. Gaumer, *supra*, at 503. One issue raised by E-Commerce through the Internet is how to apply conflicts-of-laws doctrines to lawsuits involving parties whose primary contacts with a forum and with each other have entirely been through Internet. *Id.*

6. *See* R.R. Jueneman & R.J. Robertson Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 JURIMETRICS J. 427, 433 n.26 (1998) (defining electronic as term that does not mean exclusively electrical, but includes other forms of document preparation, transmission, and storage, including fiber optic transmission lines).

7. *See* Wu, *supra* note 2, at 317 (stating that advent of E-Commerce has created need for new types of practices and suggesting as one possible practice, use of incorporating documents by reference).

8. *See Webster Hypertext Lookup* (visited Jan. 15, 1999) <http://work.ucsd.edu:5141/cgi-bin/http_webster> (on file with the *Fordham International Law Journal*) (defining authenticity to mean genuineness and quality of not being corrupted from original).

9. *See* Jueneman & Robertson, *supra* note 6, at 434 (citing concerns that concluding transactions electronically will violate current legislation that requires signed writing or that electronic documents will not be recognized as evidence in proceedings); *see also id.* at 433 n.26 (defining electronic document as digital representation of information, where human-readable characters and images have been reduced to set of binary digits, or bits, which are ones and zeros that represent those characters). The term electronic document does not refer to a stored or transmitted image of a document, such as a photographic microfilm copy or a scanned image of a document. *Id.* The difference between an electronic document and a written image of the same document is that the electronic document has captured the raw keystrokes used to create it. *Id.* In the case of a written document, the image of the document has been captured. *Id.* Electronic documents are normally stored and transmitted in computer-readable form only. *Id.*

10. Greenwood & Campbell, *supra* note 3, at 308; *see* Brian W. Smith & Timothy E.

laws that require signed and/or written records in order to create a binding legal effect.[11] Laws that require writings may range from basic contract requirements, such as the statute of frauds,[12] to other more complex provisions, such as notarization[13] and attestation.[14]

Another legally significant question involves the use, recognition, and regulation of digital signatures.[15] In addition to the numerous legal requirements for paper documents, the requirement to have a handwritten signature can be another obstruction to E-Commerce because of its effect on digital signatures.[16]

Keehan, *Digital Signatures: The State of the Art and the Law*, 114 BANKING L.J. 506, 511 (1997) (stating that threshold legal question for digital signature is whether it would be legally acceptable form of signature).

11. *See* Richard L. Field, *Digital Signatures: Verifying Internet Business Transactions*, 471 PRACT. L. INST.: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 721, 723 (Mar. 4, 1997) (stating that some laws require that certain documents must be signed by hand, specifically at bottom of document, and that original document must be used for official purposes and/or retained for specified number of years). Some concern exists that business documents might have to be admissible as valid evidence in a court of law. *Id.* Once admitted, they should have appropriate probative value. *Id.*

12. *See id.* (describing Statute of Frauds as legal provision that requires that certain documents must be in writing in order to be enforceable). The Statute of Frauds was first enacted in England in 1677 and has been incorporated into a number of areas of U.S. law at the state level. *Id.* Documents that must be in writing include contracts for the sale of goods, in excess of US$500, contracts that, by their terms, cannot be completed within one year, contracts for the sale of land, contracts that guaranty the debts of another person, agreements made in contemplation of marriage, and certain other contracts. *Id.*

13. Greenwood & Campbell, *supra* note 3, at 308; *see Webster Hypertext Lookup*, *supra* note 8 (defining notarizing as procedure when party authenticates documents).

14. *See* Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1219 (1998) (describing process of attestation when notary must determine that signature is that of person appearing before notary). The normal procedure for a notary to attest the validity of a signature is to have the person, whose signature will be notarized, appear before the notary. *Id.* The person must present to the notary sufficient evidence that the person is who he or she claims to be. *Id.* In the presence of the notary, the person will sign the document and the notary formally witnesses the signature. *Id.* The notary will affix the notarial seal or stamp and sign and date the document. *Id.*

15. *See id.* at 1198 (defining digital signature as term of art used to denote type of electronic imprint that has been produced through cryptographic procedure).

16. Randy V. Sabett, *International Harmonization in Electronic Commerce & Electronic Data Interchange: A Proposed First Step Toward Signing on the Digital Dotted Line*, 46 AM. U. L. REV. 511, 528 (1996); *see* Smith & Keehan, *supra* note 10, at 511 (arguing that threshold question for digital signatures is if they would be legally acceptable form of signature under state's statute of frauds provisions). Smith & Keehan argue that without legal recognition, electronic communications would be enforceable in court. Smith & Keehan, *supra*, at 511; *see* Richard Hill & Ian Walden, *The Draft UNCITRAL Model Law for*

Some commentators opine that written signature requirements are potentially the single greatest obstacle to E-Commerce.[17]

Many scholars note that E-Commerce will achieve its full potential only if a modern legal infrastructure exists that supports the use of digital signatures for business and government transactions.[18] They argue that an appropriate legal framework that accompanies the use of digital signatures can facilitate E-Commerce.[19] Such a legal framework can exist in a governing body of law or in private agreements that provide for the enforceability of digital signatures.[20]

Currently, a global legal framework does not exist because many nations are attempting to ensure the safety and confidentiality of their own E-Commerce transactions individually by enacting separate digital signature laws.[21] In August 1997, Germany and Italy enacted digital signature legislation, while the English, Swedish, and Dutch governments were simultaneously setting up task forces to address the creation of their own digital signature legislation.[22] In addition, many U.S. states have recently enacted

---

Electronic Commerce: Issues and Solutions, 13 No. 3 COMPUTER L.J. 18, 19 (1996) (stating that even when law does not explicitly disallow digital signatures, case law is not developed, and many businessmen are justifiably concerned about the how courts will ultimately view electronic signatures).

17. Judith Y. Gliniecki & Ceda G. Ogada, *The Legal Acceptance of Electronic Documents, Writings, Signatures, and Notices in International Transportation Conventions: A Challenge in the Age of Global Electronic Commerce*, 13 Nw. J. INT'L L. & BUS. 117, 134-35 (1992).

18. Greenwood & Campbell, *supra* note 3, at 308; *see* Scott Jensen, *AB 811 Regulates the Use of Digital Signatures in Wisconsin*, 71 WIS. LAW. 23 (1998) (explaining that although technical communications infrastructure provided by Internet is already in place, it requires continuous upgrading and expansion to keep pace with exponential growth in its use). Scott Jenson suggests that the legal and commercial infrastructure necessary to facilitate E-Commerce is less developed. Jensen, *supra*. Attorneys, business people, and policy makers are beginning to grapple with issues that need to be resolved in order for secure and binding E-Commerce transactions to become an everyday experience. *Id.*

19. *See* Sabett, *supra* note 16, at 526-27 (explaining that existing legal infrastructure embraces technology that began over 500 years ago). The present day legal infrastructure relied on paper-based systems and presents a formidable barrier to the full adoption of electronic means of conducting business. *Id.*

20. *See* Robert G. Ballen & Thomas A. Fox, *Electronic Banking Products and Services: The New Legal Issues*, 115 BANKING L.J. 334, 339 (1998) (arguing that guidelines must exist in order to enforce electronic communications, signed with digital signatures, to make them constitute writing for legal purposes).

21. Kimberly B. Kiefer, *Developments Abroad May Influence U.S. Policy on Electronic Banking*, 17 No. 4 BANKING POL'Y REP. 1, 8 (1998).

22. *See id.* at 8 (stating that in addition to these countries, Malaysia also adopted digital signature law in September 1997).

digital signature statutes that legally permit the use of digital signatures.[23]

These recent enactments have created state and national standards for regulating digital signatures that differ and sometimes conflict with one another.[24] Some countries have enacted or proposed laws that require significant state involvement.[25] Other countries have been more hesitant in enacting digital signature regulations and call for flexible standards[26] that would be easier for all countries to recognize mutually and to use.[27] Moreover, even where some laws are the same or comparable to one

---

23. *See* ARIZ. REV. STAT. ANN. § 41-121(13) (West 1998) (allowing Arizona Secretary of State to approve for and use digital signatures for documents filed with and by all state agencies); CAL. GOV'T. CODE § 16.5 (West 1997) (allowing use of digital signatures when communicating with public entity); FLA. STAT. ch. 282 § 282.70 *et. seq.* (West 1997) (setting forth Florida's Electronic Signature Act of 1996 that allows use of digital signatures for all communications); 1997 GA. CODE ANN. 40-3-21(b) (1997) (allowing commissioner to authorize use of digital signatures in car transactions); WASH. REV. CODE. ANN. § 19.34 *et seq.* (West 1998) (citing Washington Electronic Authentication Act that allows use of digital signature for all communications); *see also* Ballen & Fox, *supra* note 20, at 340 (stating that Arizona, California, Florida, Georgia, and Washington have recently enacted digital signature statutes that permit use of digital signatures). *See generally* Kiefer, *supra* note 21, at 8 (stating that 40 states legislatures are working on electronic authentication statutes).

24. Kiefer, *supra* note 21, at 8; *see* Ira H Parker, *Why Digital Signatures Matter*, 1 ELEC. BANKING L. & COM. REP. 2 (1997) (explaining current legal scenario with digital signature legislation as being formulated and debated on so many different levels, and that these different legislative approaches may raise important issues for those engaged in E-Commerce). One issue that is raised is that U.S. states bear the risk of varying and potentially conflicting standards. *Id.* This risk is compounded when entering the international arena. *Id.*

25. *See* Kiefer, *supra* note 21, at 9 (stating that Germany and Malaysia have enacted laws that entail significant governmental licensing and state involvement in digital signature regulation).

26. *See* Theodore S. Barassi, *International Developments in Digital Signature Legislation*, 2 ELEC. BANKING L. & COM. REP. 16 (1997) (describing jurisdictions such as Spain as having defined digital signature requirements with general provisions). Spain has very general, non-technically oriented provisions that establish inalterability, integrity, or uniformity of the signed electronic message. *Id.* Other jurisdictions have adopted a more detailed approach that outlines specific requirements for the use of digital signatures. *Id.*

27. *See* Kiefer, *supra* note 21, at 9 (commenting that U.S. President William Clinton's Administration wants internationally uniform regulations for digital signatures). The U.S. administration desired to pursue federal legislation to standardize the differing approaches set in place by the different states. *Id.*; *see* Mike Nelson, *White House Global Information Infrastructure—Summary of Drafting Panel Discussion* (visited Jan. 17, 1999) <http://www.whitehouse.gov/WH/EOP/OSTP/forum/html/gii.html> (on file with the *Fordham International Law Journal*) (stating that only consensus among panel of representatives from different groups, such as governmental, private, and research oriented bodies, was that effective, inexpensive, standardized global solution was urgently

another, regulators or the courts may interpret such laws in an inconsistent manner.[28] Due to this conflict of laws, some commentators have suggested that an international digital signature regime would promote E-Commerce and resolve the current conflict of laws.[29] Others have opposed any type of legislation on digital signatures, arguing that this legislation would lead to burdensome governmental regulation.[30]

This Note addresses the issue of whether all nations should enact a uniform global legal scheme governing digital signatures for the purpose of promoting E-Commerce. Part I of this Note describes digital signatures and considers their different functions. Part I also discusses E-Commerce and the application of digital signatures to E-Commerce. Further, Part I briefly examines the major legal schemes set up by organizations, states, nations, and international bodies. Part II analyzes arguments for and against global digital signature laws in order to facilitate E-Commerce. Part III argues that nations should adopt a global digital signature legal scheme in order to promote E-Commerce by eliminating conflicting laws. This Note concludes that nations should draft and enact a global digital signature legal scheme.

I. *INTRODUCTION TO DIGITAL SIGNATURES AND E-COMMERCE*

A digital signature is a way to send an encoded message to

---

needed for digital signature). The panel concluded that, otherwise, any of the potential applications of E-Commerce may not be fully developed. Nelson, *supra*.

28. *See* Ballen & Fox, *supra* note 20, at 340 (stating that some digital signature statutes are similar, but not exactly uniform among different jurisdictions). A financial institution seeking to provide electronic banking services on a multi-state basis might have to comply with potentially conflicting requirements in the different jurisdictions where it operates. *Id.* A further danger is that, even if the digital signature statutes are the same or comparable, they will be interpreted in an inconsistent manner by the jurisdiction's regulators or the courts. *Id.*

29. *See* Sabett, *supra* note 16, at 511 (opining that these domestic developments should lead to uniform international standard); *see also* Kiefer, *supra* note 21, at 13 (arguing that with current emerging network environment, information and transactions should move freely across national boundaries, and therefore governments should cooperate and coordinate policies).

30. *See* Winn, *supra* note 14, at 1181 (describing state of Internet as rapidly expanding because Internet does not have unresponsive regulatory structure). Winn argues that no compelling evidence exists that market forces are failing to create a fair and efficient result for parties. *Id.*; *see* Kiefer, *supra* note 21, at 11 (stating that some present digital signature legislation is stringent and inflexible).

another party in an electronic transaction.[31] Digital signatures can also facilitate E-Commerce by allowing parties to enter into binding contracts using the Internet.[32] Due to the importance of digital signatures to E-Commerce transactions, digital signature legislation is being formulated on individual state, national, and international levels.[33]

A. *Digital Signatures*

Using the process of cryptography,[34] a user can create a digital signature.[35] The digital signature is a string of data that is created by using asymmetric cryptography ("asymmetric").[36] Some commentators have suggested that digital signatures can serve the same legal function as written signatures.[37]

---

31. *See* Smith & Keehan, *supra* note 10, at 507 (stating that digital signature is arcane term for type of encoded message that assures each party in electronic transactions that other parties are who they say they are). Digital signatures also ensure that a received message is valid because it remains unchanged from the time of delivery. *Id.*; *see* Kiefer, *supra* note 21, at 1 (explaining digital signatures can be seen as electronic means of verifying parties that are transacting with one another).

32. *See* Jenson, *supra* note 18 (arguing that businesses have migrated to Internet and that E-Commerce has created new opportunities for banks, merchants, and consumers). Jenson states that digital signatures are an essential element for E-Commerce because they allow businesses and consumers to sign documents electronically. *Id.*; *see* Smith & Keehan, *supra* note 10, at 507 (suggesting that digital signatures may be necessary catalyst to spur E-Commerce expansion).

33. *See* Parker, *supra* note 24 (describing efforts by U.S. states, U.S. federal government, and United Nations).

34. *See* Winn, *supra* note 14, at 1198 (describing cryptography as process of taking some information, which is called the plaintext, and passing this information through an encryption process to produce encrypted copy of information, which is called ciphertext). The ciphertext can be decrypted and restored to the original plaintext through the application of the cipher key ("key"). *Id.* The key is a special type of decoder. *Id.* In general, an encryption system that uses a longer key is better protected from being broken into by outsiders. *Id.*

35. *See* Smith & Keehan, *supra* note 10, at 507 (stating that digital signature is term for encoded message that assures each party identity of other party in Internet transactions); Field, *supra* note 11, at 724 (arguing that digital signatures are an appropriate solution for E-Commerce problems).

36. *See* Greenwood & Campbell, *supra* note 3, at 313 (explaining how asymmetric, or public key cryptography works).

37. Jenson, *supra* note 18; *see* Sabett, *supra* note 16, at 523 (arguing digital signature can fulfill legal purposes of written signatures such as proving authenticity and designation of signer's approval).

1. Cryptography Principles

Cryptography is the art of communicating in secret code.[38] Two main types of cryptography are symmetric ("symmetric") and asymmetric cryptography.[39] Both cryptography systems work to change one group of symbols, which are readily readable, into another set of symbols, which are not readily readable.[40] The process of cryptography begins with a sender composing a message.[41]

a. Symmetric

Symmetric uses a single secret key[42] either to encrypt/transform a message or to decrypt/restore a message to its original form.[43] Two users must possess the same key in order to exchange messages and communicate securely with one another.[44] During the Cold War, the U.S. military used symmetric for com-

---

38. *See* Phillip E. Reiman, *Cryptography and the First Amendment: The Right to be Unheard*, 14 J. MARSHALL J. COMPUTER & INFO. L. 325, 328 (1996) (comparing process of cryptography to alphabet). Reiman states that the alphabet is a code that the public understands. *Id.* Unlike the open code of the alphabet, cryptography uses secret code in order to limit access to the contents of a message to a select group. *Id.*

39. *See* Winn, *supra* note 14, at 1199 (stating that symmetric cryptography ("symmetric") is also known as conventional or secret key and that asymmetric cryptography ("asymmetric") is also known as public key or dual key).

40. Reiman, *supra* note 38, at 328.

41. *See* National Research Council, Computer Science and Telecommunications Board, Cryptography's Role in Securing the Information Society 477 (Kenneth W. Dam & Herbert S. Lin eds., 1996) at 374 [hereinafter "CRISIS Report"] (citing example of first sender composing message for recipient and then using encryption algorithm, which is series of mathematical steps, to scramble written message).

42. *See* Reiman, *supra* note 38, at 328 (explaining how key will work). Suppose a code substitutes the original letters of a word with the letters that come two places earlier, for example Free becomes Gsff. *Id.* The process of substituting letters is known as the key. *Id.*

43. Charles R. Merrill, *Proof of Who, What, and When in Electronic Commerce Under the Digital Signature Guidelines*, 525 PRACT. L. INST.: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 129, 133 (June 24, 1998); *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, 422 (1997) (stating that computers have ability to make cryptography algorithms complex). Data can be encrypted using a special type of computer program and then decrypted using the same or a similar type of program. Wyrough & Klein, *supra*, at 422.

44. *See* Randy V. Sabett, *PGP: Securing the Privacy of Electronic Information Through Encryption*, 2 NO. 6 ELECTRONIC BANKING L. & COMPUTER REP. 13 (1997) (highlighting importance that both users possess same key in order to communicate through symmetric).

munication purposes.[45] An example of a symmetric algorithm is the Data Encryption Standard ("DES"), which the U.S. government adopted in 1977.[46] Currently, DES is the most commonly used symmetric system.[47]

The practical weakness of symmetric is keeping the key a secret.[48] Because the sender and recipient must use the same key in order to encrypt and to decrypt each other's message, they must transmit the secret key between one another.[49] A third party can intercept this transmission.[50] This problem is compounded if a user wishes to send his secret key to multiple users.[51]

b. Asymmetric

Asymmetric or public key cryptography is based on the use of two different but related keys to encrypt and decrypt messages.[52] In 1978, Ronald Rivest, Adi Shamir, and Leonard Adleman created a new style of key, the RSA system ("RSA"), which utilized two keys.[53] The sender and recipient of the elec-

---

45. *See* Winn, *supra* note 14, at 1199 (stating that U.S. military used complex logistics in order to utilize symmetric). The military used couriers that were handcuffed to locked briefcases that contained the key. *Id.* The couriers did not have the keys either to the briefcase or the handcuffs. *Id.*

46. *See* Federal Information Processing Standard 46, Data Encryption Standard, 48 Fed. Reg. 41,062 (1983) (explaining that Digital Encryption Standard ("DES") was developed by International Business Machine Corporation); *see* CRISIS Report, *supra* note 41, tbl. C1 (stating that DES uses fifty-six bit keys).

47. *See* Wyrough & Klein, *supra* note 43, at 422 (stating that experts consider DES relatively resistant to most types of attack and that DES has been extensively used in financial environments and military intelligence operations).

48. *See* Reiman, *supra* note 38, at 329 (explaining that symmetric systems require that both sender and recipient know key and that at some point these parties must exchange unencoded information about key). The communication involving information about the key is vulnerable to interception. *Id.*

49. *See* Wyrough & Klein, *supra* note 43, at 422 (stating that if sender and recipient use open data networks to exchange private keys, then possibility of compromise is great).

50. *See* Reiman, *supra* note 38, at 329 (stating that communication of secret key is vulnerable to interception).

51. *See* Sabett, *supra* note 44 (stating that symmetric suffers from security risk associated with distributing same key to all users who need to communicate with one another).

52. Winn, *supra* note 14, at 1199.

53. *See* Reiman, *supra* note 38, at 330 (stating that this system is named after its inventors and employs logarithmic function to produce two keys). A sender can choose a specific base number and an exponent to create a key that can be split between encrypting and decrypting. *Id.*

tronic message would use two mathematically generated keys, one that is public and one that is private.[54] RSA is the most commonly used method of public key encryption.[55]

With the use of two keys, public key cryptography removes most of the risks associated with symmetric key distribution.[56] In addition, parties that have never even met can use public key cryptography to send encrypted messages without the need to exchange private keys.[57] One commentator argues that public key cryptography can allow businesses to take advantage of the economic potential of the Internet.[58]

2. What is a Digital Signature?

Digital signatures are a string of data used as an electronic means of authenticating parties to a transaction.[59] Public key cryptography is the basis for creating digital signatures.[60] Although a public key corresponds with a private key, a neutral third party, known as a certification authority, ensures that the key pair is associated with the sender.[61]

---

54. *See* Wyrough & Klein, *supra* note 43, at 423 (explaining that under this system, one sender can encrypt message with recipient's public key and that recipient can use his private key to decrypt sender's message).

55. *See* Lonnie Eldridge, *Internet Commerce and the Meltdown of Certification Authorities: Is the Washington State Solution a Good Model?*, 45 UCLA L. REV. 1805, 1812 n.24 (1998) (stating that RSA has been incorporated into variety of technological applications, including Netscape's Internet Browser).

56. *See* Sabett, *supra* note 44 (stating that public key algorithms remove risk associated with private key distribution because each user can publicize his public key, for use by others in securing messages to that user).

57. *See* Wyrough & Klein, *supra* note 43, at 423 (arguing that public key cryptography resolves problems of exchanging private key and that public key cryptography can routinely make transactions that require secure communications).

58. *See* Reiman, *supra* note 38, at 331 (maintaining that because of security issues with Internet, building any business on Internet is like trying to build banks without walls). Businesses can use asymmetric systems to protect private communications and to deliver their products to consumers. *Id.* at 331-32.

59. *See* Kiefer, *supra* note 21, at 9 (stating that digital signature is created through use of private key); *see* Smith & Keehan, *supra* note 10, at 506 (defining digital signature as electronic encoded message having unique alphanumerical notation). Smith & Keehan, *supra.*

60. *See* Greenwood & Campbell, *supra* note 3, at 312-14 (stating that public and private keys make digital signatures possible); *see* Sabett, *supra* note 16, at 519-20 (explaining principles of public key cryptography are manifested in digital signatures because the structure of public/private key pair also exist in digital signature system).

61. *See* Smith & Keehan, *supra* note 10, at 508 (defining certification authority as neutral third party who issues certificate that is electronic record that represents that

a. Digital Signature Principles

The term digital signature denotes an electronic imprint that is produced using cryptography.[62] A digital signature is not a digitized[63] version of a person's handwritten signature, but rather a transformation or reduction of the text of an electronic document that is then appended to the document itself.[64] Accordingly, the recipient of a digital signature will not see the sender's signature on paper or on the computer screen.[65] Instead, the digital signature utilizes a unique alphanumerical[66] notation that guarantees the level of validity, authenticity, and security necessary to conduct electronic transactions.[67]

b. Creating a Digital Signature with Public Key Cryptography

Digital signatures are based on public key cryptography,[68] which involves the use of two codes, also known as keys.[69] The

---

signer identified in certificate is holding corresponding private key). The certification authority digitally signs the certificate and assures its authenticity. *Id.*

62. Winn, *supra* note 14, at 1198; *see* Joseph Altizer, *Electronic Signatures Authorization Act*, W. VA. LAW., Aug. 12, 1998, at 25 (stating that digital signature is transformation of electronic document into encrypted data using public key cryptography).

63. *See Webster's Revised Unabridged Dictionary* (visited Dec. 31, 1998) <http://machaut.uchicago.edu/cgi-bin/WEBSTER.sh?WORDDigitize> (on file with the *Fordham International Law Journal*) (defining digitize as process when computer converts some information, i.e. signal or image, into form expressible in binary notation).

64. Jueneman & Robertson, *supra* note 6, at 437-38; *see* Smith & Keehan, *supra* note 10, at 507 (calling term digital signature slight misnomer because it is not manual or written signature).

65. Smith & Keehan, *supra* note 10, at 507; *see* Jueneman & Robertson, *supra* note 6, at 437-38 (stating that digital signature will be appended to document); *see* Sabett, *supra* note 16, at 521 (explaining that due to mathematical basis of public key cryptography, digital signature is stream of digits that is unintelligible to human observer and that digital signature would not be displayed to user in commercial implementations).

66. *See Merriam Webster WWW Dictionary* (visited Jan. 17, 1999) <http://www.m-w.com/netdict.htm> (on file with the *Fordham International Law Journal*) (defining alphanumeric as type of text that consists of either letters or numbers or sometimes other symbols, i.e. punctuation marks and mathematical symbols).

67. Jueneman & Robertson, *supra* note 6, at 438-40; *see* Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures*, 452 PRAC. L. INST.: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 63, 67 (Sept. 1996) (explaining that digital signature is short unit of data that has mathematical relationship to data in content of document).

68. *See* Wright, *supra* note 67, at 67 (explaining that public key cryptography provides mathematical scheme for arranging any computer data, from electronic expense vouchers to medical records, such that its integrity and origin can be proven).

69. *See* Clayton J. Joffrion, *International Law*, 45 LA. BUS. J. 279, 279 (1997) (illustrating how digital signature technology uses asymmetric cryptosystem to encrypt message).

sender uses one key to authenticate the source and content of his electronic documents and the recipient uses the other key to validate that the document came from the sender.[70] In the public key cryptography system, each user is assigned two keys, a private key and a public key.[71] The private key is kept solely in the possession of the signer of an electronic document and is used to encrypt the text of the document into the digital signature.[72] The public key can be freely distributed and used by anyone.[73] The public and private keys are mathematically related, but their relationship is so complicated that it is computationally infeasible to deduce the private key solely from knowledge of the public key.[74]

Using public key cryptography, digital signature users can send messages in two ways.[75] Under one method, a message sender can use the recipient's public key to send a message to the recipient who holds the private key that corresponds to the

---

70. *See* Jueneman & Robertson, *supra* note 6, at 438 (stating that public and private keys are generated at same time); *see also* Joffrion, *supra* note 69, at 279 (stating that one party uses private key to encrypt message identifying that person). The receiving party has a public key, which can decode the private key message to identify the sender, but which can not decode the private key. Joffrion, *supra.*

71. *See* Wright, *supra* note 67, at 67 (explaining that public-key cryptography involves use of two keys, which are special strings of data). The two keys, the public key and the private key, are assigned to only one user. *Id.* Public key cryptography provides a mathematical scheme for arranging computer data through the use of these two keys. *Id.* The mathematical scheme is arranged so that the integrity and origin of the digital signature can be proven. *Id.* Each of the two keys bears a complex mathematical relationship to one another. *Id.*

72. Jueneman & Robertson, *supra* note 6, at 438; *see* Smith & Keehan, *supra* note 10, at 507 (describing private key as part of procedure to encrypt and decrypt information because it is one of two input keys). The signer should keep the private key classified. Smith & Keehan, *supra.*

73. *See* Winn, *supra* note 14, at 1200-01 (explaining that public key can be widely published and freely distributed without any compromise of private key's security). The open distribution of the public key allows parties to communicate with one another without having to find a system to distribute the keys securely. *Id.* at 1199-1200. Sender and recipient do not have to be in direct personal contact. *Id.*

74. Jueneman & Robertson, *supra* note 6, at 438; *see* Smith & Keehan, *supra* note 10, at 507 (describing keys as numerical passwords that are mathematically related, but computationally infeasible to derive from one another). This characteristic, of not being able to derive one key from the other, makes it infeasible to create a signed message that can be verified by application of the public key without a person having knowledge of the private key. Smith & Keehan, *supra.* A third party cannot identify and replicate a person's digital signature. *Id.*

75. Winn, *supra* note 14, at 1200.

public key.[76] Using another method, the message sender can use his private key to encrypt a message and send it to the recipient, who would decrypt it using the sender's public key.[77] With this method, the recipient can be certain that the message came from the sender, whose private key corresponds to the public key used to decrypt the message.[78]

The cryptography process begins when a sender wants to send a message to a recipient.[79] In order to create a digital signature, the sender must have a message to send to recipient.[80] The sender has an option to run this message through a hash function,[81] which performs a series of mathematical operations on the message.[82] The hash function creates a number that is called a message digest.[83] The sender then encodes this message digest with the recipient's public key and the result is an encrypted message.[84] The message digest, encrypted with the recipient's public key, forms the digital signature for the sender's message.[85] Next, the sender sends the message to the recipient.[86] The recipient receives the sender's message and then uses the recipient's private key to decode it.[87] During this process, neither the sender nor the recipient needs to reveal their secret

76. *See id.* (explaining that with this method, sender is assured that nobody else other than recipient, who holds the private key, will be able to read message content).

77. *See* Wright, *supra* note 67, at 67 (stating that sender can use his private key and cryptography program to attach digital signature to document). The recipient can confirm the document's authenticity by using the sender's public key and a cryptography program. *Id.*

78. Winn, *supra* note 14, at 1200.

79. Eldridge, *supra* note 55, at 1811.

80. *See* Greenwood & Campbell, *supra* note 3, at 314 (explaining that electronic message could range from simple e-mail messages to complicated lengthy contracts).

81. *See* Eldridge, *supra* note 55, at 1816 (describing hash functions as process that takes some message and produces smaller digest or message summary that is usually in form of single number). This number is unique to the message. *Id.*

82. Greenwood & Campbell, *supra* note 3, at 314.

83. *See id.* (describing message digest as message's fingerprint because slightest change in message will cause hash function to produce completely different message digest).

84. *See* Eldridge, *supra* note 55, at 1811 (stating that message is encrypted because message goes through sender's public key, and can only be decrypted by using sender's private key); Greenwood & Campbell, *supra* note 3, at 314 n.15 (explaining that message digest that was created through using hash function ensures integrity of message's content).

85. Greenwood & Campbell, *supra* note 3, at 314.

86. Eldridge, *supra* note 55, at 1811.

87. *See id.* (stating that during this process, neither sender nor recipient would need to reveal their secret keys to one another or to anyone else).

keys to one another or to anyone else.[88] This process can work using different keys.[89]

c. Public Key Cryptography Security Concerns: The Development and the Role of the Certification Authority

Public key cryptography raises several security concerns.[90] The private key must remain confidential in order to prevent another party from unauthorized use of the private key.[91] Another concern is determining whether a public key is truly associated with the party who claims to be its owner.[92] If the person uses an imposter's key, then the imposter will be able to abuse that party's information.[93]

---

88. *Id.*; *see* Greenwood & Campbell, *supra* note 3, at 311 (explaining that public key cryptography eliminates need for different users to share secret keys and that hardware and software that implements this technology shields end users).

89. *See* Eldridge, *supra* note 55, at 1815 (explaining how sender can encrypt using his private key and the recipient could decrypt with sender's public key). For example, a sender could encode a message using his private key. *Id.* By encrypting this message, the sender has produced a digital signature. *Id.* He could send this encrypted message to a recipient, who could use the sender's public key to decrypt the sender's message. *Id.* This method verifies that only the sender has sent this message because no one other than the sender can create an encrypted message that can be decrypted by sender's public key. *Id.*

90. *See* Wright, *supra* note 67, at 68 (assessing security concerns with public key cryptography, and that one such concern is that person using public/private key pair might not be proper party but imposter who stole keys). Used alone, public key cryptography does not reduce risk in signing of electronic document. *Id.*; *see* Mike Tonsing, *The Digital Certificate Comes of Age*, 45 FED. LAW 20 (1998) (describing security problems of using digital signatures alone). Suppose a lawyer receives an e-mail from his client for a copy of a privileged letter regarding prospective litigation. Tonsing, *supra*. The lawyer sends the letter to the requestor. *Id.* The requestor might not be the lawyer's client but an adverse party to the client. *Id.*

91. Winn, *supra* note 14, at 1201; *see* C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, 34 SAN DIEGO L. REV. 1225, 1236 (1997) (stating possible results of stolen private keys).

92. Winn, *supra* note 14, at 1201. *See* Eldridge, *supra* note 55, at 1813 (stating that some third party imposter can replace person's actual public key with different public key).

93. *See* Eldridge, *supra* note 55, at 1813 (describing situation that involves imposter public keys). Suppose a purchaser went to a merchant's Internet site and wanted to make a purchase. *Id.* First, the purchaser would look up the merchant's public key and then encrypt his credit card number with it. *Id.* He would send this encrypted message to the merchant. *Id.* Only the merchant would be able to read the message because the merchant would have exclusive use of its private key. *Id.* Suppose an imposter replaced the merchant's actual public key with his own key. *Id.* The purchaser would encrypt his credit card with the imposter's public key. *Id.* The imposter would be able

A public key infrastructure is a potential solution to the problem of verifying public keys to its true owner.[94] This solution involves the use of a certification authority ("CA").[95] A CA is a third party who primarily associates a public key with a particular individual.[96] The CA issues a certificate[97] that, in its simplest form, contains a copy of the public key in question and the identity of the person associated with the key.[98] One commentator has argued that CAs are important to the widespread commercial use and acceptance of digital signatures because CAs verify the identity of parties.[99] The CA may maintain an Internet directory that will contain certificates for all of its subscribers.[100]

3. Parallels Between Written Signature and Digital Signature Functions

One commentator has argued that without changing the existing paradigm of a written signature, a digital signature can ful-

---

to decode the purchaser's message using his private key and steal the purchaser's credit card number. *Id.*

94. Winn, *supra* note 14, at 1201. *See* Eldridge, *supra* note 55, at 1813 (stating that some third party that is trusted can solve problem of impostors by providing reliable directory of all its subscribers and guaranteeing that listed names and public keys are correct).

95. *See* C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L. REV. 1143, 1150 (1996) (describing certification authority ("CA") as entity that would check party's identification and take other necessary steps to assure itself that the party was indeed who they claimed); *see also* A. Michael Froomkin, *Symposium: Innovation and the Information Environment: The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 55-56 (1996) (explaining certification process).

96. *See* Smith & Keehan, *supra* note 10, at 508 (stating that CA is neutral third party that verifies public keys to make sure that it corresponds with private key and verifies association between key pair and sender).

97. *See* Biddle, *supra* note 95, at 1150 (defining certificates as digitally-signed electronic documents that attest to connection of public key to individual or other entity).

98. *See* Winn, *supra* note 14, at 1202 (stating that certificate may contain copy of person's identity, his public key, length of time certificate is valid, or any special characteristic that identifies context in which public key will be used); *see also* Eldridge, *supra* note 55, at 1813-14 (stating that certificate could contain subscriber's e-mail address or other information).

99. *See* Smith & Keehan, *supra* note 10, at 508 (positing that CAs are pivotal for widespread commercial use and acceptance of digital signatures). CAs permit parties to conduct electronic transactions without having to verify the identity of the other party independently. *Id.* Currently, several companies are vying to be CAs. *Id.*

100. Eldridge, *supra* note 55, at 1813-14; *see id.* at 1814 (stating that if private key is lost or stolen, then CA will provide certificate revocation list that identifies keys that are no longer valid).

fill all of the purposes of a written signature.[101] Traditionally, handwritten signatures have served several legal purposes—to determine authenticity, designate approval, and serve as evidence.[102] The written signature is the primary means of identifying the signer of a written document.[103] Legal analysts state that a digital signature can parallel all these purposes by its security, non-repudiation,[104] and evidentiary functions.[105]

a. Security Functions

One legal expert has stated that the digital signature provides a security function to a user because it promotes integrity[106] and authenticity.[107] The security function arises not only from the encryption process to create a digital signature[108] but also from the role of a CA to verify the identity of a party.[109] Although digital signatures make transactions more secure, they

---

101. Sabett, *supra* note 16, at 523; *see id.* at 515 (stating that digital signatures provide authenticity through its security functions). Digital signatures can provide a designation of approval through its non-repudiation function. *Id.*

102. *Id.* at 523; *see* Winn, *supra* note 14, at 1216 (defining signature as any mark or symbol that is affixed to writing to manifest the signer's intent to adopt writing and to be bound by it); Winn, *supra* note 14, at 1216-18 (listing all types of legally acceptable signatures).

103. *See* Jueneman & Robertson, *supra* note 6, at 427 (explaining that implicit assumption of why laws require written signature is that written signature identifies signer and that person's normal signature changes slowly and is very difficult to alter, erase, or forge without detection).

104. *Id.*; *see* Merrill, *supra* note 43, at 132 (defining non-repudiation as blocking false denial of both sending message and contents of message).

105. *See* Jueneman & Robertson, *supra* note 6, at 440 (stating that digital signature can be used as evidence because it has extraordinarily reliable method of validating content and sender of document).

106. *See Hypertext Webster Gateway* (visited on Jan. 17, 1999) <http://work.ucsd.edu:5141/cgi-bin/http_webster?isindex@Integrity&method@exact> (on file with the *Fordham International Law Journal*) (defining integrity "as state or quality of being entire or complete; wholeness; entireness; unbroken state"); *see also* Merrill, *supra* note 43, at 132 (referring to integrity as what were contents of message).

107. Sabett, *supra* note 16, at 515-16 (describing functions of integrity and authentication as security services that digital signatures provide user). Integrity allows messages to arrive to a recipient intact, but does not provide protection from eavesdroppers or third parties from intercepting messages. *Id.* Authentication assures the recipient that only the sender could have sent the message and is most similar to a written signature because a written signature can be attributed to its signer. *Id.*

108. *See* Smith & Keehan, *supra* note 10, at 507 (stating that public and private keys are computationally infeasible to be derived from each other); *see also* Winn, *supra* note 14, at 1200 (explaining that if sender uses his real private key in message, then recipient can only decrypt message by use of sender's public key).

109. *See* Biddle, *supra* note 95, at 1150 (describing CA as third party that checks

do not guarantee confidentiality because other parties can still intercept messages.[110] While encrypted messages can be intercepted, they cannot be read by third parties because third parties must possess the private key in order to decrypt the message.[111]

Some commentators have stated that an important function of a digital signature is to ensure integrity of the message because it verifies the accuracy of a message that has been transmitted via unsecured communications facilities such as the Internet.[112] Through this integrity function, a digital signature ensures security by assuring the recipient that the sender's message arrived intact.[113] It also provides integrity by using the hash function.[114] The hash function creates the message digest, which prevents a third party from even slightly changing the message.[115]

Analogous to a handwritten signature, a digital signature also ensures security by providing authentication.[116] Authentication, by definition, assures the recipient that only the sender could have created the message.[117] One legal analyst has stated

---

identity of subscribers and posts list of revoked public keys); *see also* Eldridge, *supra* note 55, at 1813 (stating that CAs reduce risk of imposters defrauding parties).

110. *See* Sabett, *supra* note 16, at 515 (stating that another party can still intercept message because message is transmitted in public through the Internet).

111. *See* Juan Carlos Cruellas et al., *EDI and Digital Signatures for Business to Business Electronic Commerce*, 38 JURIMETRICS J. 497, 503 (1998) (explaining that any type of message encrypted with either public or private key can only be verified or decrypted by other key). If a sender encrypts a message with the public key of the recipient, then only the private key of the recipient can decrypt the message. *Id.*

112. Field, *supra* note 11, at 724; *see* Urbaczewski et al., *supra* note 3 (stating that Internet is open and public network because it allows access to any user who uses same protocols).

113. Sabett, *supra* note 16, at 515.

114. *Id.* at 522; *see id.* at 523 (defining three characteristics of hash functions). First, a hash function must be computationally infeasible to derive another meaningful message that would result in the same message digest. *Id.* Second, it must be computationally infeasible to derive the original message from the hash value. *Id.* Third, the same results will occur for a given message and algorithm. *Id.*

115. *See* Greenwood & Campbell, *supra* note 3, at 314 (explaining that hash function is type of program that performs series of mathematical operations on message in order to create message digest number and that any change to message will create different number).

116. *See* Jueneman & Robertson, *supra* note 6, at 427 (explaining that written signature is traditional and accepted means for party to identify himself as signer of written document). Authentication enables secure transactions because it allows a party to know that it is dealing with the appropriate counter-party. *Id.*

117. *See* Field, *supra* note 11, at 724 (stating that digital signatures can authenticate

that a digital signature can go beyond the traditional role of authentication and even become a facilitator of international E-Commerce.[118] While a paper-based signature exists and authenticates either the last page or every page, if every page is initialed, a digital signature provides authentication for every character within the message.[119] The authentication function of digital signatures can eliminate the need for face-to-face meetings necessary for the signing of documents.[120] Digital signatures enable parties to prove their identities without ever having to meet.[121]

b. Non-repudiation Function

Some commentators have suggested that a digital signature serves to protect the recipient from repudiation by the sender.[122] This function ensures the recipient that the sender of the message cannot later deny having sent the message to the recipient.[123] A recipient could prove the sender's authorship by using

---

accuracy of message that has been transmitted through Internet). The CA can both authenticate the public key of a party and allocate risk of error or fraud. *Id.*

118. *See* Sabett, *supra* note 16, at 521 (stating that since digital signatures utilize sophisticated mathematical techniques, they provide security services to international E-Commerce). Sabett argues that a digital signature most importantly provides authentication for E-Commerce. *Id.*

119. *Id.*; *see* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 895 (1995) (stating that digital signature can be compared to initializing every character in message because even if message is slightly altered, message will not properly decrypt).

120. *See* Sabett, *supra* note 16, at 516 (explaining that ability to prove one's identity over great distances, without ever having met other party, can significantly increase viability of widespread E-Commerce). Sabett argues that face-to-face meetings that are required for the signing of documents will not be necessary with digital signatures. *Id.* The ceremonial aspects of signing a document will still exist; the method by which this function occurs, however, will shift from paper to electronic. *Id.* at 517.

121. *See id.* at 516 (opining that digital signature can increase viability of widespread E-Commerce because personal meetings, usually done to establish party's identity, are no longer needed); Biddle, *supra* note 91, at 1241 (stating that notion of identity is subtle concept whose nuances go to very core of human social and economic interaction).

122. Field, *supra* note 11, at 724; *see* Merrill, *supra* note 43, at 133 (explaining that non-repudiation contemplates that sender and recipient are on opposing sides of dispute). Merrill argues that non-repudiation is different from integrity and authentication because with integrity and authentication, the sender and the recipient are on the same side of the issue. Merrill, *supra*. The sender and the recipient work together to defend and to support the authenticity and integrity of a message and to prevent imposters or third parties from tampering with the message. *Id.*

123. Sabett, *supra* note 16, at 516; *see* Merrill, *supra* note 43, at 133 (describing

the sender's public key in combination with the message.[124] A digital signature strongly supports the function of non-repudiation because it is computationally unfeasible to determine the private key from the public key.[125]

c. Evidentiary Function

Finally, some experts suggest that digital signatures also serve an evidentiary function.[126] The digital signature provides reliable evidence because the received message is produced by the sender and is unchanged from the time of delivery.[127] The digital signature also provides reliable algorithmic evidence of the source of an electronically based document.[128] Experts further state that in order for digital signatures to serve as reliable evidence, the two important conditions, that the private key is kept secret and a CA is used, are met.[129]

Besides evidencing the source of a message, a digital signa-

---

situation where non-repudiation can be issue occurring when recipient attempts to defend and to support authenticity and integrity of sender's message as legally binding). The sender is attempting to repudiate his legal responsibility of the message or its contents and tries to prove that a third party sent the message. Merrill, *supra*.

124. *See* Sabett, *supra* note 16, at 522 (verifying digital signature with sender's public key, recipient has proof that only holder of corresponding private key could have created original message).

125. *See* Merrill, *supra* note 43, at 134 (stating that because of unfeasibility to derive private key from public key, any compromise of public key can only occur by person authorized to hold or have knowledge of private key).

126. Jueneman & Robertson, *supra* note 6, at 437; *see id.* at 440 (explaining that typical message digest is 160 bits in length and therefore some third party has to go through one trillion trillion messages in order to create identical message digest and therefore tamper with message). Due to this patent impossibility, the digital signature becomes irrefutable evidence that the only holder of the private key could have sent the message. *Id.*

127. Smith & Keehan, *supra* note 10, at 507; *see* Jueneman & Robertson, *supra* note 6, at 440 (clarifying conclusion that digital signature can serve as reliable evidence if identity of entity associated with public key is verified by CA and subscriber has prevented loss or compromise of private key). With these two assumptions satisfied, digital signatures are an extraordinarily reliable method of validating both the originator and the content of an electronic document. Jueneman & Robertson, *supra*.

128. *See* Jueneman & Robertson, *supra* note 6, at 438 (stating that digital signature algorithm is based on use of public and private keys and that these keys allow digital signatures created by one key to be only decrypted by other key). A document that has the digital signature, which is verified by the public key, is proof that a person possessing the private key signed it. *Id.*

129. *See id.* (explaining that party with private key must maintain secrecy and control over this key and that party depending on evidence must use reliable means of verifying identity of party with whom private key is associated).

ture is evinces that an electronic document has not been tampered with since it was sent.[130] The digital signature itself is a reduced encoding of the document.[131] If in the slightest way a document with a digital signature is altered, then the public key will fail to verify the digital signature.[132] The inability of a public key to verify the digital signature provides conclusive evidence to the recipient that the document has been altered since it was digitally signed.[133]

B. *E-Commerce*

Some experts state that E-Commerce is transforming the global economy by altering the operation of businesses.[134] Although E-Commerce is opening up new business opportunities, E-Commerce has several problems.[135] Some commentators argue that digital signatures are an appropriate solution for many of these E-Commerce problems.[136] The uses of digital signatures in E-Commerce transactions can correlate directly to the growth and development of the Internet.[137]

1. Principles of E-Commerce

The explosion of the Internet as a vehicle for consumers has made E-Commerce a current and popular topic among business circles and in newspapers. [138] Some commentators have argued

---

130. *Id.*; *see* Kiefer, *supra* note 21, at 9 (stating that process of verifying digital signature can reveal even smallest of changes in data).

131. Jueneman & Robertson, *supra* note 6, at 438.

132. *Id.*

133. *Id.*

134. Greenwood & Campbell, *supra* note 3, at 308; *see* Jensen, *supra* note 18 (stating E-Commerce revolution has spurred airlines to offer discount fare packages to consumers through Internet, banks to provide their customers with bank-at-home services, and merchants to allow consumers to shop for their goods and services on Internet).

135. *See* Urbaczewski et al., *supra* note 3 (explaining that E-Commerce transactions by themselves are not secure from actions by malicious third parties and that E-Commerce practices may not meet current legal and regulatory schemes).

136. Field, *supra* note 11, at 724; *see* Greenwood & Campbell, *supra* note 3, at 314 (stating that due to public key cryptography, digital signatures allow people and business to conduct confidential transactions over open networks). Digital signatures can enable the use of Internet systems to perform any transaction, especially transactions dealing with sensitive or official information. Greenwood & Campbell, *supra.*

137. Kiefer, *supra* note at 21, at 8.

138. Urbaczewski et al., *supra* note 3; *see* Jerry Ackerman, *Getting Fish On Line once Confined to Auction Rooms, the N.E. Industry Catches the E-Commerce Wave*, BOSTON GLOBE, Jan. 13, 1999, at C1 (reporting that New England fisheries industry have shed their low

that the current trend of E-Commerce will cause an increase in the international trade of goods and services.[139] Current investors seek public stock offerings of Internet-related companies, particularly those engaged in E-Commerce activities.[140] Some experts even suggest that certain corporations are involved or are becoming involved in E-Commerce without having a clear understanding of the reasons to engage in such transactions.[141] Other commentators suggest that E-Commerce needs greater regulation and oversight.[142] Currently, even policymakers have been focusing on regulating E-Commerce because of the emer-

---

technology reputation by putting E-Commerce and information technology to work for their needs). These fisheries are using a computer system that delivers market quotes on fish, through the Internet, to computers anywhere in the world. Ackerman, *supra*, at C1; *see India: E-Commerce Could Upset Tax Concepts*, THE HINDU, Jan. 7, 1999 (reporting that popular use of E-Commerce can upset existing direct and indirect tax principles). Foreign vendors can sell products to another country, without establishing a physical presence in that country, and can avoid local source taxation. *India: E-Commerce Could Upset Tax Concepts*, *supra*.

139. Don Macleod, *From the Editor . . . Virtual Jurisdiction*, 2 NO. 8 INTERNET LEGAL RESEARCHER 2, (1997); *see* Jennifer Conovitz, *A Framework for Global Electronic Commerce*, 1075 PRAC. L. INST.: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 11, 13 (Sept. 1998) (stating that Internet technology is making profound effect on global trade in services and certain goods). Conovitz estimates that current world trade involving computer software, entertainment products, information, and professional services account for over US$40 billion of U.S. exports alone. Conovitz, *supra*.

140. *See* Dunstan Prial, *Bounty of Internet IPOs in U.S. Present a Few Pros Among '.coms'*, ASIAN WALL ST. J., Jan. 5, 1999, at 20 (stating that U.S. Securities and Exchange Commission has received many initial public offering applications from companies whose names end with .com and are related to Internet). Prial also suggests that Priceline.com, Inc. is an example of a corporation that engages in E-Commerce and is expected to be another promising public stock offering. *Id.* Priceline.com is managed by Richard Braddock, former president of Citicorp, and has been backed by Microsoft Corporation's co-founder Paul Allen. *Id.*

141. *See* Richard Blackwell, *E-Commerce Strategies Unclear: Report*, NAT'L POST, Sept. 10, 1998, at 8 (stating that some financial service institutions are putting more resources into E-Commerce initiatives without proper planning or vision on how E-Commerce will increase profit). Blackwell suggests that some banks are allocating resources to E-Commerce plans only because they are just following their competitors. *Id.* Fifteen Canadian financial institutions that were surveyed spend, on average, nine percent of their information technology budget on E-Commerce, compared to the three percent average of financial institutions as a whole. *Id.*

142. *See* Meg Fletcher, *Electronic Commerce Needs Regulators' Attention: Survey*, BUS. INS., Jan. 4, 1999, at 21 (reporting that National Association of Insurance Commissioners conducted online survey in which members voiced that state insurance regulators must continue to identify and overcome existing E-Commerce barriers for insurance industry).

gence of its use through the Internet.[143]

The current discussion on E-Commerce underlies existence of E-Commerce, which has been in use for many years.[144] Some commentators have suggested that early organizations that used telephones and telegraphs to communicate with one another engaged in E-Commerce.[145] In the 1950s, businesses increasingly began to use computers and this emergence of computer use opened new opportunities for commercial applications.[146] Then in 1969, the U.S. Department of Defense created the Internet as a project to facilitate the exchange of information among educational institutions and governmental agencies.[147] The Internet has since become a universal appliance for every day life and has become accessible from almost anywhere in the world.[148] E-Commerce needs a communication network to support it, so the evolution of the Internet has caused the present increase in E-Commerce transactions.[149]

Although the Internet may seem to have limitless potential, especially in the area of E-Commerce, some experts have noted that the use of the Internet for E-Commerce has some

---

143. Urbaczewski et al., *supra* note 3; *see* Greenwood & Campbell, *supra* note 7, at 307-08 (stating that growth of E-Commerce affects every sector of economy and this growth has attracted attention of policy makers). Greenwood & Campbell argue that these policy makers believe that E-Commerce can achieve its full potential if a modern legal infrastructure supports the use of online services for business and government transactions. Greenwood & Campbell, *supra*, at 308.

144. *See* Urbaczewski et al., *supra* note 3 (stating that E-Commerce has already been in use through different technologies, such as automated teller machine transfers, e-mail, fax, interactive telephone, telegraph, and telex).

145. *Id.*

146. *See id.* (explaining that computers assist business in numerous ways, such as freeing time for business manager to strategize for new products and markets, to expedite communication process, to clear geographic hurdles, and to allow rapid globalization of businesses).

147. *See* Gaumer, *supra* note 5, at 503 (stating that Internet exists because millions of separate computer operators decided to use common protocols to exchange communications and information with other computers).

148. *See* Conovitz, *supra* note 139, at 13 (stating that Internet used to be solely reserved for scientific and academic exchange, but is now being used by people for different purposes, one of which is to reinvent government because Internet is becoming outlet for personal and political expression). Conovitz also states that businesses are participating in the Internet and are developing new models of consumer interaction. *Id.* Entrepreneurs can easily start new enterprises because they use the Internet's worldwide network of consumers and have lower start up costs. *Id.*

149. *See* Urbaczewski et al., *supra* note 3 (stating that E-Commerce is nothing without communications network to support it and that evolution of Internet has shaped present growth of E-Commerce).

problems.[150] E-Commerce transactions take place over the Internet, which is an open and unsecure network, and thus another party can intercept the information in these transactions.[151] Another problem for E-Commerce is that the Internet infrastructure needs to develop and grow to accommodate the increased amount of online users.[152]

2. Uses of Digital Signatures in E-Commerce

Experts suggest that digital signatures may be the catalyst necessary to spur the expansion of E-Commerce.[153] Digital signatures can be used as an electronic means of authenticating the identities of parties to a transaction.[154] The use of digital signatures can correlate directly to the growth and development of the Internet.[155] One group has stated that the Internet is a novel business environment because it is an open, global network of computers.[156] The Internet has grown rapidly since its incep-

---

150. *See* James Hill, *Lock and Load Document Security on the Net*, BUS. L. TODAY, Dec. 8, 1998, at 8 (stating that one problem of Internet is that it has significant amount of crime). A potential exists for greater incidents of civil fraud on the Internet. *Id.*

151. *See* R.J. Robertson Jr., *Electronic Commerce on the Internet and the Statute of Frauds*, 49 S.C. L. REV. 787, 796 (1998) (explaining that messages sent through Internet are not sent over one pathway, but transmitted over series of thousands of networks and can be read by third parties). A message must move, using intermediary packet switching nodes, from one network to another before reaching its final goal. *Id.* Any person with access to any intermediate node can alter, read, or intercept a message in a way that is undetectable by the recipient. *Id.*

152. *See* Urbaczewski et al., *supra* note 3 (explaining that when amount of user traffic exceeds bandwidth of particular network, network becomes very slow as amount of messages queue up to be delivered through network lines). The commentator states that currently less than one percent of world's population is connected to the Internet. *Id.* If an additional ten percent became connected, then the Internet infrastructure could collapse. *Id.* E-Commerce would also become slowed or even die out. *Id.*

153. Smith & Keehan, *supra* note 10, at 507.

154. *See* Field, *supra* note 11, at 724 (stating that digital signatures can be used to authenticate accuracy of message and can also authenticate sender of message).

155. Kiefer, *supra* note 21, at 8.

156. *See* Winn, *supra* note 14, at 1183 (explaining how Internet is open in four ways). The National Research Council has noted that the Internet is open in at least four ways. *Id.* First, the Internet is open to all users because it does not force users into closed groups or deny access to any group in society. *Id.* Second, it is open to service providers because it allows an open and accessible environment for competing commercial interests. *Id.* Third, it is open to network providers because any network provider can satisfy the necessary requirements to attach and to become part of the aggregate of interconnected networks. *Id.* Fourth, it is open to change because it constantly permits the introduction of new applications, services, and technologies and is not limited to only one application, for example television. *Id.*

tion, both in terms of computer capability and the number of Internet users.[157] The U.S. government has asserted that electronic networks, like the Internet, allow people to transcend barriers of time and distance to take advantage of global markets and business opportunities and to open a new world of economic possibility and progress.[158] Currently, many businesses are starting to capitalize on the Internet and are conducting E-Commerce transactions.[159] The banking industry is an example of an area where digital signatures are being used to process E-Commerce transactions.[160]

Besides being used by the banking industry, commentators agree that digital signatures can be utilized in any situation with any two parties that wish to contract.[161] For example, this technology could be used to close a business deal[162] or to conduct any type of official or sensitive transaction otherwise done on

157. *See id.* at 1187 (citing statistics relating to Internet growth). The number of host computers—those that relay communications and store data—increased from about 300 in 1981 to approximately 9.4 million by 1996. *Id.* About 40 million people used the Internet in 1996, a number that is expected to mushroom to 200 million by 1999. *Id.*

158. *See* President William J. Clinton & Vice-President Al Gore, Jr., *A Framework for Global Electronic Commerce*, July 1, 1997 (visited Feb. 6, 1999) <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (on file with the *Fordham International Law Journal*) (stating that United States is on verge of revolution with Internet). Electronic networks allow people to transcend time and distance barriers to take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress. *Id.*.

159. *See* Gaumer, *supra* note 5, at 503 (stating that businesses are not only advertising on Internet, but also are using digital signatures to consummate E-Commerce transactions). The Home Shopping Network, Inc. has created an Internet Shopping Network. *Id.* Companies such as Ford, Wal-Mart, Merrill Lynch, Pizza Hut, Xerox, J.P. Morgan, General Electric, JC Penny, and Target have used the Internet to reach customers and do business with them. *Id.*

160. *See* Smith & Keehan, *supra* note 10, at 506 (stating one application of digital signatures is by some large and small financial institutions that have introduced home banking services to their customers). These services offer an array of personal conveniences such as inquiring account information, applying for credit card, paying bills, transferring funds between different accounts, and purchasing one or more of the institution's deposit and non-deposit products. *Id.* Smith and Keehan have predicted the widespread use of Internet banking by the year 2000. *Id.*

161. Winn, *supra* note 14, at 1207; *see* Merry Mayer, *USPS to Use PKI to Offer Electronic Postage*, NEWSBYTES, Sept. 10, 1998 (reporting that U.S. Postal Service ("USPS") will use public key infrastructure services in order to sell postage over Internet). The USPS's public key infrastructure will ensure secure transaction for online buyers. *Id.*

162. *See* Sabett, *supra* note 16, at 512-13 (using hypothetical that two businesses, which are located in different countries, may conduct complex deals by using digital signatures).

paper.[163] By using digital signatures, the Internet can be used as a means of communication between any type of party that wants to enter into contracts with any other type of party.[164] Because the Internet is unsecure, parties without a pre-existing business relationship will be more reluctant to enter into contracts through the Internet than will parties who are familiar with one another.[165] Digital signatures allow all people and businesses to use the Internet fully for E-Commerce.[166]

C. *Present Legal Digital Signature Schemes*

Many localities, nations, and global organizations have enacted or are considering the enactment of laws governing the use of digital signatures.[167] Some of these laws address the many legal and technical issues surrounding digital signatures differently than others.[168] A brief discussion of some of the major digital signature legal schemes can provide useful background information with respect to the question of whether all nations should adopt a global digital signature scheme.

1. U.S. Initiatives Regarding Digital Signatures

Commentators state that traditionally in the United States, issues of enforceability and authenticity of signatures and agree-

163. *See* Greenwood & Campbell, *supra* note 3, at 314-15 (giving examples of transaction that can be done through Internet, such as sending and receiving tax returns, making purchase orders, sending mortgage applications, or applying for and accepting credit card applications).

164. Winn, *supra* note 14, at 1207.

165. *See id.* (discussing problems of interaction between unknown parties). Parties with a pre-existing business relationship can create authentication procedures that build on their own existing policies and procedures. *Id.* Parties soliciting new business over the Internet have bigger security concerns that are harder to resolve because they are not accustomed to dealing with one another. *Id.*

166. *See* Field, *supra* note 11, at 724 (stating that public key cryptography, upon which digital signatures are based, gives parties high degree of certainty that their communications are confidential, authentic, and accurate). These characteristics of digital signatures are needed in order to conduct business transactions in an open environment like the Internet. *Id.* This level of security is far greater than the security provided by a written signature. *Id.*

167. *See* Barassi, *supra* note 26 (stating that there is high level of United States and non-U.S. legislative activity in recognizing digital signature use).

168. *See* Kiefer, *supra* note 21, at 9 (discussing different types of state intervention for enacted digital signature laws). Nations such as Germany and Malaysia have enacted laws that call for a heavy state role in the licensing of certification authorities. *Id.* The U.S. state of Utah enacted a law that does not involve heavy government regulation. *Id.*

ments are primarily governed by state and not federal law.[169] It follows that a number of states have placed their faith in digital signature technology and have adopted laws that recognize and regulate the use of digital signatures.[170] For example, Utah was the first jurisdiction to enact legislation regulating digital signatures.[171] Utah received assistance from the American Bar Association's[172] ("ABA") Information Security Committee[173] ("Committee"), which was the first organization that attempted to deal with digital signature issues systematically.[174]

a. The ABA Digital Signature Guidelines

The ABA created the ABA Digital Signature Guidelines ("Guidelines") because no legal precedents existed governing

---

169. *See* Ballen & Fox, *supra* note 20, at 339 (stating that because U.S. states legislate directly on signatures, different initiatives are underway in U.S. states to provide greater degree of legal certainty and predictability with respect to digital signatures).

170. *See* TEX. GOV'T CODE ANN. § 403.027 (West 1997) (setting forth Texas law that allows use of digital signatures, but is limited to transactions with Texas State Comptroller or between Public Agencies); *see also* VA. CODE ANN. §§ 59.1-467-469 (Michie 1997) (amended 1998) (setting forth Virginia law that allows use of digital signatures and is applicable for all communication). *See generally* Kiefer, *supra* note 21, at 1 (stating that some states have enacted digital signature legislation and more than 40 state legislatures have begun to work on electronic authentication laws); McBride, Baker, Coles, *Scope of Authorization to use of Electronic Signature in Enacted Legislation* (visited Jan. 17, 1999) <http://www.mbc.com/ds_sum.html> (on file with the *Fordham International Law Journal*) (giving summary of enacted digital signature statutes).

171. *See* UTAH CODE. ANN § 46-3 (1995) (setting forth Utah Digital Signature Act that authorizes digital signature use for all communications); *see* Maureen S. Dorney, *Digital Signature Legislation*, 491 PRACTICE L. INST.: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 141, 157 (Sept. 1997) (stating that in May 1995 Utah enacted comprehensive legal framework for digital signatures to allow for their widespread use and adoption in E-Commerce).

172. *See American Bar Association Profile Page* (visited Jan. 16, 1999) <http://www.abanet.org/media/overview/pintro.html> (on file with the *Fordham International Law Journal*) (describing American Bar Association ("ABA") as national organization of legal profession in United States). The ABA is composed principally of court administrators, business executives, government officials, judges, lawyers, and law professors. *Id.*

173. *See Information Security Committee Home Page* (visited Jan. 17, 1999) <http://www.abanet.org/scitech/ec/isc/home.html> (on file with the *Fordham International Law Journal*) (explaining purpose of Information Security Committee). Since 1992, the Information Security Committee ("Committee") has been the source of E-Commerce legal initiatives. *Id.* The Committee deals with current computer security issues including cryptology, public key infrastructure, risk analysis, and the legal efficacy of secure digital commerce. *Id.*

174. Winn, *supra* note 14, at 1239; *see* Dorney, *supra* note 171, at 157 (stating that several members of Committee even drafted sample digital signature statute for Utah legislature).

the use of digital signatures.[175] The Guidelines are general statements of principles.[176] Ultimately, the substantive rules of the Guidelines establish interrelated legal duties for CAs, parties using CAs, and any person relying on digital signature certificates.[177]

i. Legislative History and Purpose of the ABA Guidelines

Prior to the ABA's work on digital signature laws, the ABA was defining the legal boundaries of E-Commerce.[178] This study examined the effects of E-Commerce upon fundamental principles of contract law and related legal issues and led to the development of a Model Electronic Data Interchange Trading Partner Agreement and Commentary ("Model TPA").[179] Although the Model TPA did not change the paradigm in requiring a signature, it allowed the parties considerable flexibility in defining what type of signature is acceptable.[180]

During the late 1980s and early 1990s, businesses began to recognize the potential for using public key cryptography in commercial transactions.[181] No legal precedents existed regarding transactions using a public key infrastructure.[182] Due to the absence of any established legal guidelines, the Committee set out to address this problem and eventually drafted the Guidelines.[183] In 1992, the Committee began work on a project that

175. Winn, *supra* note 14, at 1240.

176. *See* AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE, 20 (1996) [hereinafter GUIDELINES] (stating Guidelines are intended as "a common framework of unifying principles that may serve as a common basis for more precise rules in various legal systems").

177. *Id.* at 18.

178. Sabett, *supra* note 16, at 531; *see* Michael S. Baum et al., *Model Electronic Data Interchange Trading Partner Agreement and Commentary*, 45 BUS. LAW 1645, 1718 (1990) (explaining that in 1987, Electronic Messaging Services Task Force, under auspices of ABA, began study on E-Commerce regulation, which was in response to absence of clear legal guidance regarding E-Commerce).

179. Baum et al., *supra* note 178, at 1718.

180. *Id.* at 1731; *see* Sabett, *supra* note 16, at 531 (noting that existing technology, sophistication of parties, and applicable standards must be taken into consideration when deciding which digital signature technology to use).

181. Winn, *supra* note 14, at 1240.

182. *See id.* (arguing that this lack of legal guidance had chilling effect on development of commercial applications of public key cryptography because users could not build business models involving digital signatures).

183. *Id.*

culminated in the 1996 creation of the final version of the Guidelines.[184] A large number of attorneys and technologists drafted the Guidelines.[185] These drafters were familiar with public key cryptography and realized that the potential commercial utilization of this technology would take place only when some of the legal uncertainty surrounding its implementation had been resolved.[186]

ii. Substantive Provisions of the Guidelines

The Guidelines do not purport to be a model law.[187] Instead, the Guidelines offer general statements of principle regarding the development of public key infrastructures, with the intent of influencing the development of more exact rules within various legal systems.[188] The Guidelines have been influential in the United States and in the international development of public key infrastructure thinking.[189] The Guidelines have also formed the basis for digital signature legislation in a number of U.S. states.[190]

The drafters of the Guidelines had several objectives in attempting to eliminate the uncertainty involving the use of digital signatures.[191] One of the objectives was to create a legal framework within which risks of potential liability to digital signature

184. Field, *supra* note 11, at 725.

185. Winn, *supra* note 14, at 1240.

186. *Id.*

187. *See* Guidelines, *supra* note 176, at 19-20 (stating that ABA Guidelines are not intended for adoption as text for statute or regulation because they are not suitable for that purpose). The Guidelines recommend that legislators should resolve issues left open in the Guidelines by implementing a digital signature legal and institutional infrastructure for digital signatures. *Id.*

188. *See id.* at 19 (stating that Guidelines are general statements of principle). They are intended as a common framework of unifying principles that can serve as a common basis for precise rules for other legal systems. *Id.*.

189. Field, *supra* note 11, at 725.

190. *See id.* (stating that Utah was first state to pass law authorizing use of digital signatures in commerce in UTAH CODE ANN. § 46-3-102 (1995)). The Utah legislation makes extensive references to the Guidelines. *Id.*

191. *See* Guidelines, *supra* note 176, at 18 (stating that Guidelines seek to establish safe harbor for use of digital signatures). The drafters of the Guidelines wanted to create a secure computer-based signature equivalent in order to accomplish four goals. *Id.* They sought to minimize incidence of electronic forgeries, to foster reliable authentication of documents in computer form, to facilitate commerce by means of computerized communications, and to give legal effect to technical standards for authentication of computerized messages. *Id.*

developers could be kept within tolerable limits.[192] The drafters of the Guidelines also attempted to set forth the type of legal infrastructure needed for a system in which third parties could act as CAs.[193]

Under the Guidelines, a CA must disclose digital signature certificates and provide available information regarding the revocation of certificates to relying parties.[194] When deciding to issue a digital signature certificate, CAs must screen the online identity of the certificate's recipient.[195] The Guidelines do not instruct the CA on how to make the decision to issue a certificate beyond requiring that it disclose in its certification practice statement the procedures that it will follow.[196] The Guidelines also fail to mention any active monitoring by the CA of the continued validity of any of the information provided by a certificate's recipient.[197] According to the Guidelines, a CA must maintain a trustworthy system[198] and guarantee that its employees and contractors support the system's maintenance.[199] The certificate's recipient must safeguard the private key that corresponds to the public key in the certificate.[200]

---

192. *See id.* (requiring developers to use X.509 directory standard and certain patented encryption technology in order to get benefits of this reduced liability). Winn, *supra* note 15, at 1241.

193. Winn, *supra* note 14, at 1241-42.

194. *See* Guidelines, *supra* note 176, § 3.12 (stating that CAs must promptly publish notice of suspension or revocation if certificate was published and must disclose fact of suspension or revocation on inquiry by relying party); *see also id.* § 1.27 (defining relying party as "person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them"); Winn, *supra* note 15, at 1241-42.

195. *See* Guidelines, *supra* note 176, § 3.7 (listing representations in certificate); *see* Comment to Guidelines 3.7.1 (stating that § 3.7 does not require CA to guarantee or underwrite factual accuracy of confirmed information). The Comment to the Guidelines ("Comment") suggests that the level of investigation required can vary. *Id.* § 3.7.1.

196. *See* Guidelines, *supra* note 176, § 3.2 (listing disclosure requirements).

197. *See id.* § 3.11 (describing when CA should revoke or suspend without consent of subscriber).

198. *See id.* § 1.35 (defining trustworthy systems as when all computer hardware, software, and procedure must be "reasonably secure from intrusion and misuse; provide a reasonably reliable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and adhere to generally accepted security principle"); *see also id.* § 3.1 (stating that CA must have trustworthy systems).

199. *See id.* § 3.4 (stating that "CA must formulate and follow personnel practices which provide reasonable assurance that the trustworthy system of the CA is supported by the performance of duties of employees and contractors on behalf of the CA").

200. *See id.* § 4.3 (stating that "during the operational period of a valid certificate,

The Guidelines provide that if a CA has complied with these rules, then it is not liable for any losses incurred by a subscriber[201] or by a relying party.[202] This limit on the CA's potential liability is a risk allocation rule.[203] The Guidelines' drafters introduced this type of liability allocation scheme because they were concerned that courts might entertain the claims of subscribers or relying parties against CAs.[204] In addition, the lack of legal precedent regarding the duties of CAs created an undesirable ambiguity from the point of view of potential CAs.[205]

Although the Guidelines reduce some ambiguity for parties and developers interested in digital signatures by providing a legal framework, one commentator suggests that the Guidelines are vague in certain areas because they do not offer parties clear definitions.[206] Another vague issue is the legal capacity of parties entering into a contract.[207] Also, the Guidelines do not offer

---

the subscriber shall not compromise the private key corresponding to a public key listed in certificate, and must also avoid compromise during any period of suspension"); *see* Comment, *supra* note 195, 4.3.2 (stating that standard of care for safeguarding of private key should be higher than standard of care imposed by federal law on credit card or Automatic Teller Machine cardholders).

201. *See* Guidelines, *supra* 176, § 1.31 (defining subscriber as person who "is the subject named or identified in a certificate issued to such person and holds a private key that corresponds to a public key listed in that certificate").

202. *See id.* § 3.14 (listing all types of liability from which CA is free if CAcomplies with the Guidelines).

203. *See* Winn, *supra* note 14, at 1242 (stating that this provision excludes any liability that CA assumes unless it has expressly assumes more risk in its certification practice statement); *see also* Comment, *supra* note 195, 1.8.2 (elaborating that certification practice statement may contain duties of CA to relying person).

204. *See* Winn, *supra* note 14, at 1242 (explaining that drafters feared that CAs will be liable even when no contractual privity exists between CA and relying party or in spite of contractual terms that attempt to bind subscriber to terms of CA's certification practice statement). Such courts might hold the CA liable for some or all damages. *Id.*

205. *See id.* (stating that case law, drawn from analogous situations, was not favorable to CAs' position); *see also* Kline v. First Western Government Securities, Inc, 24 F.3d 480 (3d Cir. 1994) (holding that law firms can not limit its liability to investors if it stated in opinion letter that letter was for exclusive use of investment firm).

206. *See* Winn, *supra* note 14, at 1243 (stating that Guidelines do not concretely define what is trustworthy system for CA). In addition, it might be possible to define what makes a trustworthy system for a CA in reference to other guidelines developed in financial services and military contexts. *Id.* It is unclear what is an appropriate level of security for an individual using public key cryptography for personal or household use on an individual personal computer. *Id.*

207. *See id.* at 1244 (stating that Guidelines do not address situation when other party is business organization rather than natural person). The Guidelines also do not address issues regarding the ability or inability of the other party to fulfill its contractual undertaking. *Id.*

legal guidance regarding possible conflicts of law.[208] The Guidelines also assume that the CA will neither put any effort into learning about the subscriber's circumstances, nor make any meaningful disclosure to the subscriber regarding the appropriate level of security procedures that the subscriber should use.[209]

b. The Utah Digital Signature Act

With the assistance of the Committee, the U.S. state of Utah developed its own digital signature legislation.[210] One of the purposes of this legislation is to promote E-Commerce.[211] The substantive provisions of the Utah legislation create a liability structure for digital signature use, make certain legal presumptions about digital signatures,[212] and impose detailed duties on all parties to a digital signature transaction.[213]

i. Legislative History of the Utah Digital Signature Act

In 1995, Utah became the first jurisdiction in the world to enact comprehensive legislation governing the implementation and use of digital signatures for E-Commerce.[214] Utah developed this legislation in collaboration with the Committee.[215] Some members of the Committee drafted a sample digital signature statute for the Utah legislature even before the Guidelines were complete.[216] This collaboration resulted in the enactment

208. *See id.* (affirming belief that contracting parties in E-Commerce transaction need to have information and legal guidance regarding possible conflicts of laws). For example, if the parties do not live in the same jurisdiction, they bear the risk of being brought into court in a remote and hostile jurisdiction for any dispute arising out of the transaction. *Id.*

209. *Id.* at 1247.

210. Biddle, *supra* note 91, at 1232-33; *see* Dorney, *supra* note 171, at 157 (explaining that some members of Committee assisted Utah legislature in drafting digital signature statute).

211. *See* UTAH CODE ANN. § 46-3-102(1) (1995) (stating purpose of Utah Act is "to facilitate commerce by means of reliable electronic messages").

212. *See* Smith & Keehan, *supra* note 10, at 510 (explaining that Utah Act apportions, creates, and limits liability of CA, public key-private key holder, and party who relies on certificate).

213. *See* Biddle, *supra* note 91, at 1232 (arguing Utah Act imposes duties on CAs, digital signature users, and parties that rely on digital signatures).

214. Smith & Keehan, *supra* note 10, at 509-10.

215. Biddle, *supra* note 91, at 1232-33.

216. Dorney, *supra* note 171, at 157.

of the Utah Digital Signature Act ("Utah Act").[217] Following enactment, nearly a dozen states proposed digital signature legislation that closely resembled the Utah Act.[218] The Utah Act has also been influential at the international level.[219]

The drafters of the Utah Act intended to facilitate E-Commerce by promoting the use of digital signatures on computer-based documents.[220] Commentators state that the Utah Act allows various types of personal and commercial transactions to be performed online.[221] The Utah Act also provides a comprehensive digital signature legal framework, which the drafters felt would be sufficient to allow the widespread adoption and use of digital signatures in E-Commerce.[222] It created a legal infrastructure in which users employ repositories,[223] CAs, and public-key encryption technology to sign electronic documents in a legally binding fashion.[224] Additionally, the Utah Act intended

---

217. *See* UTAH CODE ANN. § 46-3 (1995) (setting forth Utah Act, which applies to use of digital signatures in all applications); Biddle, *supra* note 91, at 1232-33.

218. *See* Biddle, *supra* note 91, at 1233 (stating relationship between Washington and Minnesota digital signature laws and Utah Act). In 1997, Washington and Minnesota enacted laws that closely tracked the Utah Act. *Id.* California rejected using the Utah Act as a model, but early drafts of the California law closely followed it. *Id.*

219. *See id.* (listing countries that have looked at Utah Act for guidance). Malaysia enacted legislation based upon the Utah Act. *Id.* Australia, Canada, Germany, Singapore, the European Union (or "EU"), and the United Nations Committee on International Trade Law have utilized the Utah Act in their proposed or enacted legislation. *Id.* at 1233-34.

220. *See* UTAH CODE ANN. § 46-3-102(1) (1995) (stating one purpose of Utah Act is to facilitate commerce by means of electronic messages that are reliable).

221. *See* Smith & Keehan, *supra* note 10, at 510 (explaining some permissible and potential transactions through use of Utah Act). These transactions include purchases of financial products, the filing of tax returns, and submissions of applications for approval. *Id.* Utah authorities are working together with private groups to facilitate electronic transactions by using digital signatures. *Id.* The state has been involved in the recently founded Utah Electronic Law Project, a private initiative that attempts to advance the transition to electronic commerce by the end of the year. *Id.*

222. *See* UTAH CODE ANN. § 46-3-102 (1995) (stating purposes of Utah Act). Part I of the Utah Act states that its goal is to effectuate the four following purposes. *Id.* First, the Utah Act is to facilitate commerce by means of reliable electronic messages. *Id.* Second, the Utah Act is to minimize the incidence of forged digital signatures and fraud in E-Commerce. *Id.* Third, the Utah Act implements legally the general import of relevant standards, such as X.509 of the International Telecommunication Union. *Id.* Fourth, the Utah Act establishes, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages. *Id.*

223. *See id.* § 46-3-103(29) (defining repository as "system for storing and retrieving certificates and other information relevant to digital signatures").

224. *See id.* § 46-1-103(10) (defining digital signature as "transformation of a

digital signatures to use hash functions.[225]

ii. Substantive Provisions of the Utah Act

Under the Utah Act, a digital signature is as valid as if it were written on paper.[226] A document with a digital signature creates a rebuttable legal presumption that the message sender intended to be legally bound by its contents.[227] In addition, a digital signature that satisfies the criteria of the Utah Act will satisfy any Utah rule of law requiring a written signature.[228] This provision eliminated the need to expressly amend each Utah statute that has a writing or signature requirement.[229] Furthermore, the Utah Act gives documents that are signed with digital signatures legal status similar to that of notarized documents.[230]

In addition to giving legal status to digital signatures, the Utah Act maintains that the state will act as the main CA and will be in charge of licensing CAs.[231] The Utah Department of Com-

---

message using an asymmetric cryptosystem"); *see also id.* §§ 46-3-301–310 (listing duties of CA and subscriber).

225. Biddle, *supra* note 95, at 1143.

226. *See* UTAH CODE ANN. § 46-3-403 (stating that digital signature is "as valid, enforceable, and effective as if it had been written on paper, if it" meets two requirements). The message must "bear in its entirety a digital signature." *Id.* Finally, the digital signature must have been "verified by the public key listed in a certificate" that was validly issued by a licensed CA at the time the digital signature was created. *Id.*; Dorney, *supra* note 171, at 157.

227. *See* UTAH CODE ANN. § 46-3-406(3)(b) (1995) (presuming that signer of digital signature affixed the digital signature with intention of signing message); *see also* Dorney, *supra* note 171, at 157-58 (stating that in order for this provision to be applicable, digital signature is verified by reference to public key listed in valid certificate issued by licensed CA).

228. *See* UTAH CODE ANN. § 46-3-401 (1995) (allowing digital signatures to satisfy rule of law that requires signatures or provides consequences in absence of signature). Digital signatures can satisfy a law requiring a written signature if it satisfies three requirements. *Id.* The digital signature must be verified by reference to the public key listed in a valid certificate issued by a licensed CA. *Id.* The signer must affix the digital signature with the intention of signing the message. *Id.* Finally, the recipient must not know that the signer breached a subscriber duty or does not rightfully hold the private key used to affix the digital signature. *Id.*

229. Dorney, *supra* note 171, at 158.

230. *See* UTAH CODE ANN. § 46-3-405 (1995) (stating that "certificate issued by a licensed CA is an acknowledgment of a digital signature verified by reference to the public key listed in the certificate"). This status is given "regardless of whether words of an express acknowledgment appear with the digital signature or whether the signer physically appeared before the CA when the digital signature was created, if that digital signature is verifiable by that certificate and affixed when that certificate was valid". *Id.*

231. *See* Utah Act § 46-3-201(2) (requiring Division to issue licenses for CAs).

merce will directly regulate CAs.[232] The Utah legislature used this scheme in order to give users confidence to utilize digital signatures as a viable authentication procedure for E-Commerce transactions.[233]

The Utah Act also outlines the responsibilities of a CA.[234] It limits who can qualify as a licensed CA.[235] A licensed CA must post a bond or letter of credit.[236] The Utah Act also sets forth adequate record keeping procedures and provides for the regular audit of CAs.[237] Moreover, the Utah Act sets out the procedure that CAs must follow when they cease to act as a CA or when they issue, revoke, or suspend a certificate.[238] The Utah Act specifies certain information that must be included in the certificate.[239] Licensing under the Utah Act is voluntary, yet licensed CAs are offered limited liability as a legal benefit for becoming licensed under the act.[240]

One expert has argued that the liability scheme is one of the most analyzed parts of the Utah Act.[241] The Utah Act im-

---

232. *See id.* § 46-3-103(11) (defining Division as Division of Corporations and Commercial Code within Utah Department of Commerce).

233. *See* Winn, *supra* note 14, at 1202 (explaining situation on how parties can rely on CA). Winn argues that one method of reliance is to setup another type of CA, called a root CA, who would certify other CAs. *Id.* The problem is creating a root CA that will give confidence to parties to use digital signatures as a viable authentication procedure in E-Commerce applications. *Id.* The Utah legislature enacted legislation that authorized the state to act as the root CA and to provide for the licensing of CAs. *Id.*

234. *See* UTAH CODE ANN. § 46-3-301 (1995) (delineating duties of CA). A CA can issue, suspend, or revoke a certificate. *Id.* A CA must give notice on the issuance, suspension, or revocation of a certificate. *Id.* A CA can create a private key. *Id.*

235. *See id.* § 46-3-201 (listing licensing requirements for CAs). The CA must not employ anyone convicted of fraud. *Id.* § 46-3-201(1)(b). The CA must maintain an office in Utah or have a registered agent for service of process. *Id.* § 46-3-201(1)(g). A party involved in the Utah Act must be the subscriber of a certificate that is published in a recognized repository, which is defined in Utah Act § 46-3-501. *Id.* at § 46-3-201(1)(a).

236. *See id.* § 46-3-201(1)(d) (requiring CAs to file suitable guaranty with Division); *see also id.* § 46-3-103(34) (defining what satisfies surety guaranty).

237. *See id.* § 46-3-202 (setting forth procedure on how CA will be audited).

238. *See id.* § 46-3-302 (setting forth procedure on how CA will issue, revoke, or suspend certificate).

239. *See id.* § 46-3-103(3) (stating that certificate is computer based record that identifies CA who issued it, names the subscriber, contains subscriber's public key, and is signed digitally by CA who issued it). *Id.*

240. Biddle, *supra* note 91, at 1233.

241. *See* Biddle, *supra* note 95, at 1193 (stating that Utah Act's liability provision allocates risks to parties using digital signatures and is extensively studied by CAs and consumers).

poses a standard of care on CAs that is comparable to the negligence standard imposed on notaries, but with some notable deviations.[242] When a CA complies with the duties articulated in the Utah Act, the CA enters the safe harbor provision under the Utah Act that shelters them from liability.[243] The Utah Act directly limits the liability of licensed CAs in two ways; one method is that if the CA complied with the Utah Act then it is not liable for losses by a false or forged digital signature.[244] Under the second method, the Utah Act limits the liability for licensed CAs for their errors or negligence to the amount specified in the certificate.[245]

Some experts argue that the Utah Act also indirectly protects CAs through its liability scheme regarding digital signature users.[246] Consumers who participate in the public key infrastructure under the Utah Act subject themselves to a great risk of liability.[247] Under the Utah Act, the user whose private key was used to sign a document has unlimited liability if he failed to use reasonable care to protect his private key.[248] The Utah Act creates certain rebuttable presumptions in disputes involving the

---

242. *See id.* at 1180 (explaining difference with notary model). Once a forgery has been shown, the notary model shifts the burden of persuasion in a dispute over a forged acknowledgement or signature. *Id.* Once a plaintiff shows that a signature is forged, the burden shifts to the notary who must prove that it exercised the proper standard of care. *Id.* The Utah Act has no similar provision. *Id.*

243. *See* UTAH CODE ANN. § 46-3-309(2)(a) (1995) (stating that licensed CA is not liable for any reliance loss caused by false signature of subscriber if CA complied with all material requirements). The CA is also not liable over "the amount specified in the certificate as its recommended reliance limit for either a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed CA is required to confirm or failure to comply with § 46-3-302 in issuing the certificate." *Id.*; *see* Biddle, *supra* note 95, at 1180 (explaining liability structure in Utah Act). The Utah Act states that certification authorities shall not be liable for any loss that is caused by reliance on a false or forged digital signature of a subscriber if the CA complied with all the material requirements. Biddle, *supra.*

244. *See id.* § 46-3-309(2)(a) (stating that CAs may not be liable for false or forged digital signatures). A CA is not liable for any loss that is caused by reliance on a false or forged digital signature if the CA complied with all the requirements. *Id.* A CA can waive this protection. *Id.*

245. *See id.* § 46-3-309(1) (specifying CA's limit to damages because CA is not liable for any reliance losses, punitive or exemplary damages, and pain and suffering damages).

246. Biddle, *supra* note 91, at 1236.

247. Biddle, *supra* note 95, at 1144.

248. *See* UTAH CODE ANN. § 46-3-305(1) (1995) (stating that subscriber identified in certificate assumes duty to exercise reasonable care to retain control of private key).

user and the CA.[249] The user must present to a court clear and convincing evidence to overcome these presumptions.[250] For example, suppose a licensed CA issues a certificate to a subscriber.[251] Suppose a subscriber has his private key stolen by a third party[252] and the third party uses the private key to cash a $30,000 electronic check drawn from the user's account prior to the private key's revocation.[253] In court, the user must overcome the presumption that the electronic check signed with his digital signature is valid and binding upon him.[254] If the user fails to overcome this presumption, then he must bear the $30,000 loss.[255]

2. International Initiatives

Many nations have enacted or are in the process of enacting digital signature laws.[256] Germany became the first European nation to enact a comprehensive digital signature law.[257] In addition, the European Commission ("Commission" or "EC") has proposed a directive on digital signatures similar to the German legislation.[258]

---

249. *See* Biddle, *supra* note 95, at 1168 (stating presumptions set forth by Utah Act). The Utah Act instructs courts to presume that if a digital signature is verified by the public key listed in a certificate validly issued by a licensed CA, then there are three consequences. *Id.* The subscriber has accepted the corresponding certificate and therefore has assumed the duty to exercise reasonable care to protect his private key. *Id.* The digital signature belongs to the subscriber listed in the certificate. *Id.* Finally, the digital signature was affixed with the intention of signing the message. *Id.*

250. *See* Biddle, *supra* note 91, at 1236 (describing the clear and convincing standard as being higher than usual mere preponderance of evidence standard in civil cases); *see also* Biddle, *supra* note 95, at 1168-69 (explaining how digital signatures have higher standard of proof). Under the Utah Act, digitally signed documents are considered acknowledged documents. Biddle, *supra* note 86. The burden of proof for an acknowledged document is that a party needs clear and convincing evidence. *Id.* This standard is more onerous than the mere preponderance of the evidence. *Id.*

251. Biddle, *supra* note 95, at 1169.

252. Biddle, *supra* note 91, at 1236.

253. Biddle, *supra* note 95, at 1169.

254. *Id.* at 1170.

255. *Id.*

256. *See* McBride Baker & Coles, *Summary of Electronic Commerce and Digital Signature Legislation* (visited Jan. 17, 1999) <http://www.mbc.com/ds_sum.html> (on file with the *Fordham International Law Journal*) (summarizing U.S. state, U.S. federal, and international initiatives on digital signatures).

257. Kiefer, *supra* note 21, at 11.

258. *See id.* (stating that United States encouraged development of voluntary, market-driven key management infrastructure that could perform integral functions of au-

a. The German Act

On July 22, 1997, Germany enacted the *Gesetz zur digitalen Signatur*, or the Act on Digital Signature ("German Act").[259] Article 3 of the Federal Information and Communication Services Act embodies the German Act.[260] The German Act sets out a framework for the safe use of digital signatures in business transactions over the Internet.[261]

i. Legislative History of the German Act

One commentator states that the enactment of the German Act indicated that Germany's political leaders intended to facilitate legal certainty in the area of digital signatures.[262] German lawyers practice and train in the Civil Code system and therefore must derive legal guidance from codified law.[263] German policymakers quickly draft new legislation when they discover an unregulated area.[264] The German Civil Code already provides that most agreements do not require a written form.[265] The drafters of the German Act established these regulations in order to make Internet transactions using digital signatures more secure.[266]

ii. Substantive Provisions of the German Act

The German Act defines digital signatures and sets forth the

---

thentication, integrity, and confidentiality). The German law and the new EU Directive incorporate these ideas. *Id.*

259. Gesetz zur digitalen Signatur (Signaturgesetz), v. <22.7.1997> (BGBl. I S. 1870, 1872); Kiefer, *supra* note 21, at 11

260. Informations und Kommunikationsdiente Gesetz (Kommunikationsdientegesetz), 37 I.L.M. 564 (1998); Heiner Buenting, *The New German Multimedia Law—A Model For the United States*, 14 No. 9 COMPUTER LAW. 17, 17 (1997).

261. Kiefer, *supra* note 21, at 11.

262. Buenting, *supra* note 260, at 21.

263. *Id.* at 17; *see Central Intelligence Agency World Factbook: Germany*, (visited Jan. 4, 1999) <http://www.odci.gov/cia/publications/factbook/gm.html> (on file with the *Fordham International Law Journal*) (giving overview on Germany and stating that Germany has civil law system with judicial review of legislative acts in Federal Constitutional Court).

264. Buenting, *supra* note 260, at 17.

265. *Id.* at 18.

266. *See* Gesetz zur digitalen Signatur (Signaturgesetz), v. <22.7.1997> (BGBI. I S. 1870, 1872) § 1(1) (stating that "[t]he purpose of this law is to create conditions for digital signatures under which they may be deemed secure and forgeries of digital signatures or falsifications of signed data may be reliably ascertained").

roles of the involved parties.[267] In addition, it contemplates the use of public key cryptography.[268] As defined in the German Act, a digital signature seals and labels digitized data that is intended for electronic transmission.[269] A certifier,[270] or CA, gives the user a private digital signature.[271] A user's participation under the German Act is voluntary because the Act does not require users to use a digital signature from a licensed CA.[272]

Participation under the German Act by CAs is also voluntary.[273] The German Act allows the central government to set up a licensing scheme for CAs.[274] The government gives this power to the German Telekom authority,[275] which can grant a license to any applicant who is reliable and has the necessary expert knowledge.[276] The CA must also implement a detailed and approved security plan setting forth all security measures, the technology utilized, and an organizational flowchart.[277]

---

267. *See id.* § 2(1) (defining digital signature); *see also id.* § 3 (defining state involvement); *id.* § 4 (describing licensing process for CAs).

268. *See id.* § 2(1) (stating that digital signature is seal that "digital data created with a private signature key, which seal allows, by use of the associated public key to which a signature key certificate of a [CA] or of the Authority under § 3 is affixed, the owner of signature key and unforged character of data to be ascertained").

269. Buenting, *supra* note 260, at 18.

270. *See* Signaturgesetz, § 2(2) (defining certifier as "natural or legal person which attests to the attribution of public signature keys to natural persons and holds a license therefore under Seciton 4").

271. *See id.* § 5(1) (stating that CA "shall reliably identify persons who apply for a certificate"); *see also* Buenting, *supra* note 260, at 18 (obtaining license requires that applicant be identified). The use of a pseudonym with the digital signature is allowed. Buenting, *supra*, at 18.

272. *See* Buenting, *supra* note 260, at 18-19 (stating that German government hopes that technical standards set in German Act will become generally accepted).

273. *See* Christopher Kuner, *Commentary to the German Digital Signature Law* (visited Jan. 17, 1999) <http://www.kuner.com/data/sig/digsig4.htm> (on file with the *Fordham International Law Journal*) (stating that while German Act is voluntary, German government wants to create *de facto* standard for use of digital signatures); *see also* Kiefer, *supra* note 21, at 11 (stating that compliance with German Act is purely voluntary). Businesses may choose to proceed within the German Act when using digital signatures and certificates. Kiefer, *supra*, at 11.

274. *See* Gesetz zur digitalen Signatur (Signaturgesetz), v. <22.7.1997> (BGBl. I S. 1870, 1872) § 3 (stating that granting of licenses under German Act rests with German government).

275. *See id.* § 4(1) (requiring certifiers to be licensed by Telekom Authority).

276. *See id.* § 4(2) (requiring that license given to certifier shall be denied if factual ground exists that applicant does not have reliability necessary to be certifier or does not have expert knowledge for operation to be certifier); *see also id.* § 4(3) (defining requirements of reliability and expert knowledge).

277. *See* Kiefer, *supra* note 21, at 11 (stating that German Telekom Authority rigor-

Under the German Act, the CA's main responsibility is to issue digital certificates.[278] The CA's technology must conform to certain performance standards.[279] For example, the technology must guarantee that subscribers have a functioning key pair and a tool that keeps the private key secret.[280]

In certain situations, the German Act gives digital signatures legal effect.[281] An example of the enforcement of digital signatures is when parties agree to their use in a contract.[282] Other types of contracts still require a written signature.[283]

The German Act also addresses the issue of reciprocity with digital signatures from other countries.[284] The German Act provides for mutual recognition of digital signature certificates from other European Union ("EU") Member States, as long as those States are judged to have an equivalent security level.[285] A non-EU country must be party to an agreement with Germany in order to receive reciprocity for the other country's digital signatures.[286] Germany has not yet signed a treaty with the United

---

ously analyzes these three requirements). The CA must report to the Telekom Authority every two years on continuing compliance with the German Act and its regulations. *Id.*

278. *See id.* (explaining that to obtain certificate, private persons must enter private services contract with CAs).

279. *See id.* (stating that standards are based on International Information Technology Security Evaluation Criteria and Information Technology Security Evaluation Manual).

280. *See id.* (requiring that key pair be unique). It must be impossible to either duplicate the private key or to derive the private key from knowing the public key. *Id.* The technology being used must keep the private key secret. *Id.*

281. *Id.*

282. *See id.* (stating that when parties agree to use digital signatures, these contracts are enforceable under German Act).

283. *See id.* (explaining that under German law, transactions in real property transactions, wills, long-term leases and certain loan securities require written signatures).

284. *See* Gesetz zur digitalen Signatur (Signaturgesetz), v. <22.7.1997> (BGBl. I S. 1870, 1872) § 15(1) (stating that non-German certificates "with a public key signature for which a foreign certificate of another Member State of the European Union or of another Contracting State of the Treaty on the European Economic Area exists are equivalent to digital signatures under this law, insofar as they demonstrate an equivalent level of security"); *id* § 15(2) (stating that certificates from "other States, insofar as supranational or international agreements concerning the recognition of certificates have been concluded").

285. *See id.* § 15(1) (allowing digital signature certificates from EU Member States if they are equivalent to digital signatures under German Act and have equivalent level of security).

286. *See id.* § 15(2) (applying same response for non-EU nation if it has treaty with Germany for digital signatures).

States regarding the acknowledgement of U.S. digital signatures.[287]

The German Act does not address other areas of concern, such as the liability of using digital signatures.[288] The German Act also does not specify whether digital signatures can be used as evidence in a court proceeding.[289] By itself, a digital signature will not meet the standards of documentary evidence but may have some probative value if introduced as evidence in court.[290]

b. EC Draft Directive on Digital Signatures

One expert has opined that the Commission legislation is similar to the German Act. [291] The Commission, however, proposed a digital signature guideline that would create minimum rules concerning security and liability and ensure that digital signatures are recognized legally throughout Europe based on the principles of the Single Market.[292] The proposed legislation covers a range of legal topics under digital signatures.[293]

i. Legislative History of the Commission Draft Directive

On October 8, 1997, the Commission adopted a communication that recommended creating a European Framework for digital signatures ("Communication").[294] The purpose of the

287. Buenting, *supra* note 260, at 19.

288. *See* Kiefer, *supra* note 21, at 11 (stating that traditional concepts of German contract and tort law govern liability issues).

289. Buenting, *supra* note 260, at 18.

290. *See id.* (explaining that digital signatures lack required physical form for under Section 415 of the German Civil Procedure Code). This obstacle could be overcome because the German Civil Procedure Code allows production of evidence if there is judicial inspection. *Id.*

291. *See* Kiefer, *supra* note 21, at 11 (stating that both German Act and European framework are voluntary and both provide for mutual recognition for digital signatures within European Union). Kiefer argues that the German Act can be expected to be a model for European Union. *Id.*

292. *See* Heather Rowe, *European Commission's Proposal for an 'Electronic Signatures' Directive*, 3 CYBERSPACE LAW. 10 (1998) (describing principle of Single Market as free movement of services and home country control within Europe).

293. *See id.* (stating that Commission legislation is in technology neutral language and that this legislation defines basic requirements for digital signatures, creates liability framework, gives legal effect to digital signatures, describes certification measures, and includes mechanisms for cooperation with non-EU countries).

294. European Commission, Ensuring Security and Trust in Electronic Communication: Toward a European Framework for Digital Signatures and Encryption, COM (97) 503 (Oct. 1997) [herinafter Communication].

Communication was to establish and to develop a European legal framework for digital signatures.[295] The drafters of the Communication also wanted to provide parties with the security and trust necessary for the use of digital signatures.[296] Experts have stated that the lack of security on electronic networks, such as the Internet, is one of the major obstacles impeding the development of E-Commerce.[297] The Communication covered numerous areas with respect to digital signatures.[298] On May 13, 1998, the Commission followed the Communication with a draft proposal on a Common Framework for Electronic Signatures ("Draft Directive").[299] The Draft Directive establishes a *de minimis* set of rules concerning liability and security and ensures that digital signatures are legally recognized throughout the European Community.[300] The Draft Directive is considered timely because certain European Community Member States have enacted or are in the process of enacting digital signature legislation.[301]

---

295. *See* Communication, *supra* note 294, COM (97) 503, at 2 (defining goals of Ensuring Security and Trust in Electronic Communication ("Communication")). The Communication stated that a European framework for digital signatures should be established, which would ensure the functioning of the Internal Market for cryptographic products and services and stimulate a European industry for these products. *Id.* Another goal of the Communication is to remove barriers for cryptographic services and products, thus enabling all economic sectors to benefit from the opportunities of a global information society based on a framework of trust. *Id.*

296. *See id.* at 1 (explaining that first part of Communication emphasized authentication and integrity services because they are essential for secure and trustworthy data transmission and communication over all open networks). "In order to make good use of the commercial opportunities offered by electronic communication via open networks, a secure and trustworthy environment is therefore necessary." *Id.* "Digital signatures can help to prove the origin of data (authentication) and verify whether data has been altered (integrity)." *Id.*

297. Rowe, *supra* note 292; *see* Kiefer, *supra* note 21, at 10 (explaining that any EU legislation is part of overall initiative by policymakers to promote security for E-Commerce transactions, especially for transactions involving financial services).

298. *See* Communication, *supra* note 294, COM (97) 503, at 2-5 (discussing and defining digital signatures, certification process, key management, mutual recognition in different countries, privacy, legal problems, liability, legal recognition of digital signatures, and regulatory considerations).

299. European Commission, Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures, COM (98) 297 Final (May 1998) [hereinafter Draft Directive]; *see* Rowe, *supra* note 292 (citing one of its main supporters, Mr Martin Bangemann, who stressed that ability to conduct secure E-Commerce is essential to stimulate use of E-Commerce).

300. *See* Rowe, *supra* note 292 (explaining that principles of mutual recognition of digital signatures throughout European Union follow Single Market principles).

301. *See id.* (referring to Mr. Mario Monti of the European Commission, who has

ii. Substantive Provisions of the Draft Directive

The Draft Directive begins by setting forth the requirements of a digital signature.[302] The directive also sets forth the requirements for digital signature certificates.[303] Under the Draft Directive, all digital signatures are given full legal effect, even when they are not based on a qualified certificate or issued by an accredited CA.[304] A digital signature that meets the Draft Directive requirements satisfies laws that require a written signature and is admissible as evidence in legal proceedings.[305] Furthermore, the Draft Directive also defines other components and parties involved in the use of digital signatures.[306]

The Draft Directive refers to CAs as certification service providers ("CSPs").[307] CSPs must follow certain requirements.[308] CSPs that comply with the Draft Directive have a set liability provision.[309]

---

agreed that proposal is timely because most Member States have not set up legislative framework for digital signatures). Mr. Monti stated that this proposal can ensure a harmonious legal framework for the Single Market from the outset instead of having to counter potentially disparate national initiatives. *Id.*

302. *See* Draft Directive, *supra* note 299, COM (98) 297 Final, art. 2(1) (defining electronic signature as signature in digital form that is either attached to or logically associated with data that is used by a signatory to indicate their acceptance of the content of that data).

303. *See* Rowe, *supra* note 292 (defining these requirements). The Commission of the European Communities wanted to ensure a minimum level of security and free movement throughout the Single Market. *Id.* These requirements are not technical in nature. *Id.* Policy makers wanted the Draft Directive to be technology neutral. *Id.*

304. *See* Draft Directive, *supra* note 299, COM (98) 297 Final, art. 5(1) (requiring Member States not to deny legal effect, validity, and enforceability solely because signature is in electronic form, not based upon qualified certificate, or not based upon certificate issued by accredited certification service provider).

305. *See id.* art. 5(2) (stating that digital signatures are admissible only in same manner as handwritten signatures).

306. *See id.* art. 2(2)-(7) (defining signature creation device, signature verification device, qualified certificate, certification service provider, electronic signature product).

307. *See id.* art. 2(6) (defining certification service providers as entity or person that issues certificates or performs other services related to digital signatures to public).

308. *See id.* annex II (listing requirements for CAs such as demonstrating reliability necessary for offering certification services, operate prompt and secure revocation service, and verify through appropriate means identity and capacity of person that a certificate will be issued).

309. *See* Draft Directive, *supra* note 299, COM (98) 297 Final, art. 6 (explaining that CA would be liable only to person who reasonably relies upon certificate in four instances). Under the Draft Directive, the CA would be liable for the accuracy of all information in the qualified certificate as of the issuance date, unless stated otherwise by the CA. *Id.* A CA would have to comply with all the requirements of the European

Digital signatures that comply with the Draft Directive can circulate freely throughout the Internal Market.[310] Articles 3 and 4 of the Draft Directive deal with the treatment of digital signature legislation by Member States.[311] The Draft Directive prohibits restrictions on certification services that originate from other Member States.[312] The Draft Directive also contains a mechanism for recognizing digital signature certificates from other countries.[313]

II. *ARGUMENTS FOR AND AGAINST A GLOBAL REGULATORY SCHEME FOR DIGITAL SIGNATURES: WHAT IS IN THE BEST INTEREST OF E-COMMERCE?*

Many jurisdictions have enacted digital signature legislation that either recognizes or regulates digital signature use.[314] Some commentators suggest that legislators create digital signature laws and business people support them because both groups want to protect and to nurture E-Commerce.[315] As a result of

---

Directive in the certificate. *Id.* A CA must ensure that the party identified in the qualified certificate held the signature creation device that corresponds to the signature verification device given or identified in the certificate. *Id.* A CA must also assure that the signature verification device and the signature creation device both work in a complementary manner. *Id.*

310. *See id.* art 4(2) (allowing digital signature products that comply with Directive to circulate freely through internal market).

311. *See id.* art. 3 (discussing market access stating that "Member States shall not make the provision of certification services subject to prior authorization"); *see also id.* art. 4 (discussing Internal Market Principles); *id.* art. 3(2) (stating that "Member States may introduce or maintain voluntary accreditation systems aiming at enhanced levels of certification service provision"). These schemes must be objective, proportionate, non-discriminatory, and transparent. *Id.* § 3(2).

312. *See id.* art. 4(1) (restricting Member States from prohibiting certification services from other Member States).

313. *See id.* art. 7(1) (specifying how to deal with non EU certificates). A certificate issued by a non-EU certification service provider will be legally equivalent to certificates by an EU member in three ways. *Id.* The CA can fulfill the requirements of the European Directive and become accredited by a Member State. *Id.* A CA, established in the Community and who fulfills the requirements of the European Directive, guarantees the non-EU CA to the same extent as its own certificates. *Id.* Finally, the certificate or CA is recognized under a bilateral or multilateral agreement between the Community and third countries or international organizations. *Id.*

314. *See* Barassi, *supra* note 26 (stating that U.S. states, Argentina, Chile, Denmark, Germany, Italy, Malaysia, and EU have already drafted digital signature legislation).

315. *See* Greenwood & Campbell, *supra* note 3, at 307-08 (stating that growth of E-Commerce affects every sector of economy). This growth has attracted the attention of policy makers and they realize that E-Commerce can achieve its full potential if a mod-

these different laws, proponents of a global regulatory scheme for digital signatures argue that such a scheme will promote E-Commerce by providing certainty and guidance and by eliminating currently conflicting laws.[316] Opponents of a global regulatory scheme for digital signatures argue that such a scheme will inhibit E-Commerce transactions with a burdensome regulatory structure.[317]

A. *Arguments for a Global Regulatory Scheme for Digital Signatures Will Promote E-Commerce*

Proponents of a global scheme for regulating digital signatures argue that such a scheme promotes E-Commerce.[318] They argue that not only will a global scheme promote E-Commerce by providing certainty about the legal effect of transactions using digital signatures, but also that such a scheme may provide guidance to parties in the use of digital signatures.[319] They also argue that conflicting digital signature laws must be eliminated in order to allow flow of goods and services from E-Commerce transactions.[320]

The Internet supports many types of transactions and these transactions can take place between well-established clients or strangers.[321] Some experts state that the digital signature is the

---

ern legal infrastructure supports the use of online services for business and government transactions. *Id.*

316. *See* Parker, *supra* note 24 (arguing that because digital signature legislation is being created on so many different levels, parties engaging in E-Commerce have to deal with many important issues, one of which is conflicting standards).

317. *See* Winn, *supra* note 14, at 1253 (arguing that interest groups are pressuring their legislatures to devise regulatory scheme before full maturation of E-Commerce).

318. *See* Sabett, *supra* note 16, at 525-26 (arguing that for E-Commerce revolution to occur, legal framework is need to delineate liabilities, responsibilities, and rights of parties involved). Sabett further argues that international E-Commerce cannot occur on a vast scale unless a law provides clarity with respect to E-Commerce. *Id.*

319. *See* John F. Olson et al., *Letter from the Editors: State Legislation Lags Market and Technology*, 2 No.2 WALLSTREETLAWYER.COM: SEC.ELEC.AGE 2 (1998) (describing problem with U.S. state digital signature legislations). States have either not adopted legislation that recognizes digital signatures or have enacted non-uniform laws. *Id.*

320. *See* Kiefer, *supra* note 21, at 9 (noting that many nations have enacted conflicting standards and that some of these standards have been criticized as being overly burdensome to E-Commerce).

321. *See* Greenwood & Campbell, *supra* note 3, at 314-15 (showing that tax returns, mortgage applications, and other complicated agreements can be carried out through Internet); Winn, *supra* note 14, at 1207 (explaining difference in treatment of known and unknown parties in conducting E-Commerce transactions). Parties who have pre-existing business relationships can agree upon authentication procedures. Winn, *supra.*

necessary catalyst to expand E-Commerce.[322] They argue that digital signatures can guarantee a high level of validity, authenticity, and security necessary to conduct faceless electronic transactions.[323] They further argue that in order to fully utilize digital signatures, nations must enact appropriate legal framework.[324] Some experts conclude that international E-Commerce transactions cannot occur on a large scale unless a global regime is set in place that provides adequate clarity and guidance for conducting transactions.[325]

1. Global Regulatory Scheme for Digital Signatures Will Promote Legal Certainty in International E-Commerce Transactions

Proponents argue that the absence of a global legal infrastructure for digital signatures is an enormous barrier to widespread E-Commerce.[326] Presently, no international rules governing digital signatures exist.[327] Although numerous states, nations, and regional organizations have enacted digital signature legislation, many policy makers recognize the need for international cooperation in creating a global regulatory scheme for digital signatures.[328]

Parties face great uncertainty when they conduct transac-

Parties wishing to solicit new business have greater security concerns. *Id.* These security and authentication problems can be resolved using digital signatures. *Id.*

322. Smith & Keehan, *supra* note 10, at 507.

323. *Id.*

324. *See* Ballen & Fox, *supra* note 20, at 339 (arguing that this framework can be either in governing body of law that provides for the enforceability of electronic documents signed with digital signatures, and/or in private agreements). Ballen & Fox further argue that if a governing body of law is enacted, a digital signature must be recognized as a writing. *Id.*

325. *See* Sabett, *supra* note 16, at 526 (arguing that legal framework can help parties in E-Commerce transactions). Legal commentators argue that in order for the revolution to occur, a legal framework must be erected that will delineate the rights, responsibilities, and liabilities of the various parties involved. *Id.* at 525-26; *see* Dorney, *supra* note 171, at 160 (arguing that in order to foster E-Commerce growth, governments and private sector should work together to adopt comprehensive legal framework for digital signature use).

326. *See* Field, *supra* note 11, at 724 (discussing confusion and hesitation among parties who wish to engage in E-Commerce transactions, but fear that they will be subject to unknown risks or that their transaction will be illegal).

327. *See* Winn, *supra* note 14, at 1179 (explaining that commercialization of Internet has opened debate on how E-Commerce transaction should be regulated and has also caused many jurisdictions to pass their own digital signature laws).

328. Kiefer, *supra* note 21, at 9; *see id.* at 13 (arguing that despite agreeing on

tions using digital signatures.[329] With the lack of international regulatory guidance, many issues are left unresolved.[330] One such question experts have asked is, in terms of cross-border transactions, what is the legal status to be accorded to certificates from CAs from other nations with different regulatory schemes.[331] Legal scholars opine that the various digital authentication legislative efforts have added more uncertainty for an international business.[332] These varied legislative efforts not only indicate a legal landscape comprised of varied treatment of digital authentication issues, but also creates uncertainty for the future of E-Commerce.[333] Some legal scholars argue that these issues must be addressed to allow digital signatures to assist in the expansion of E-Commerce.[334]

---

necessity of international uniform standards, countries are still developing their own standards and are thus more interested in shaping than adapting to global standards).

329. *See* Dorney, *supra* note 171, at 150 (describing situation of applying written signatures laws, when digital signatures are used, as creating great uncertainty). A digital signature is a technical concept. *Id.* Its legal significance will depend on whether it is a signature under the applicable law. *Id.* Under current law in most jurisdictions, the legal effect of a digital signature would be determined by looking at the circumstances surrounding a transaction, such as whether the party applying the digital signature intended to be legally bound. *Id.* It is possible that a digital signature would be found to be a signature under either current common law or statute. *Id.* The result is uncertain. *Id.*

330. *See id.* at 150-51 (listing unresolved issues such as who, if anyone, should license or regulate CAs; what should be scope of such regulation; what are responsibilities of CAs; and what are consequences when a party loses control over its private key).

331. *Id.*; *see* Parker, *supra* note 24 (arguing that because digital signature legislation is being formulated on different jurisdictional levels, those engaging in E-Commerce are at risk of violating these enactments because of varying and potentially conflicting standards, especially in international transactions); *see also* Kiefer, *supra* note 21, at 8 (describing current legal situation in United States because United States currently has no federal legal scheme regarding digital signatures and over 40 state legislatures have considered or are considering this issue).

332. *See* Barassi, *supra* note 26, at 16 (listing nations that have drafted proposed statutes or regulations that deal with specific issues in regards to digital signature technology). Barassi argues that current digital signature legislation efforts throughout the world will disappoint an international business that seeks a predictable legal environment within to conduct E-Commerce. *Id.* Also, regional organizations, such as the European Community and the Asia Pacific Economic Cooperation, are in the process of enacting standards. *Id.*

333. *Id.*

334. *See* Sabett, *supra* note 16, at 525-26 (stating that in order for E-Commerce revolution to occur, legal framework must be erected that delineates liabilities, responsibilities, and rights of various parties involved). Proponents argue that international electronic transactions cannot occur on a more frequent and vaster scale unless the law provides adequate clarity. *Id.*; *see* Jueneman & Robertson, *supra* note 6, at 433-34 (stating that electronically concluding contracts raise legal question on how to establish

2. Global Regulatory Scheme for Digital Signatures Will Assist in Developing Uniform Digital Signature Standards

Proponents of a global regulatory scheme for digital signatures argue that the development of this scheme will promote E-Commerce by assisting countries to develop their own digital signature standards.[335] This scheme could resolve technical issues by simply establishing a globally-accepted standard.[336] Proponents argue that, taken as a whole, a global regulatory scheme for digital signatures can promote E-Commerce because it would recognize and support the entire digital signature infrastructure.[337]

Some experts have stated that a well-formulated statutory scheme can provide guidance to business persons, programmers, courts, and regulators, and therefore ultimately facilitate transactions on the Internet and promote E-Commerce.[338] For example, the law could encourage the growth of this system because it would recognize the interaction between users and CAs.[339] This recognized standard would also promote secure transactions, which will increase E-Commerce.[340] Some commentators note

---

genuineness of E-Commerce transactions because these transactions consist solely of streams of ones and zeroes). Legislators have attempted to reform existing legal requirements for written documents in order to give legal recognition to electronically signed documents. Jueneman & Robertson, *supra*.

335. *See* Smith & Keehan, *supra* note 10, at 507 (arguing that global law is critical for conduct and consummation of financial and other E-Commerce transactions).

336. *Id.*; *see* Sabett, *supra* note 16, at 533 (explaining that harmonized law or set of guidelines can apply to all areas of digital signatures). Some experts state that for the technology to reach its fullest potential, progress must be made at all levels of the law. Sabett, *supra*, at 533. The clarification of details of digital signature use will widely implement E-Commerce and make it be used effectively. *Id.*

337. *See* UTAH CODE ANN. § 46-3-102(1)-(3) (1995) (stating that Utah Act is intended to facilitate commerce by means of reliable electronic messages and to implement uniform standards).

338. *See* Smith & Keehan, *supra* note 10, at 507 (giving example of commercial and retail customers who would be able to purchase financial institution's products and services and to execute binding legal obligations over Internet).

339. *See* Jueneman & Robertson, *supra* note 6, at 443-44 (stating that legally recognizing users that have private and public keys and that use CAs would promote secure E-Commerce transactions). Users could enter into binding contracts by using a private and public key. *Id.* A CA could provide the parties with verification that they are dealing with the proper parties. *Id.* More users would enter into binding contracts with this system in place. *Id.*

340. *See* Eldridge, *supra* note 55, at 1813 (stating that more consumers can go to merchants' Internet sites and purchase items by using their credit card because consumers will be assured that transaction is secure).

that the surge in Internet activity indicates that the development of legal standards and protections that enforce electronic transactions and electronic signatures are still in the embryonic stage.[341] One recent report on Internet activity shows that E-Commerce will quickly and prematurely level off if comprehensive laws are not enacted to define the parameters for enforceable and valid electronic transactions and agreements.[342]

3. A Global Regulatory Scheme for Digital Signature Will Promote E-Commerce by Eliminating the Current Conflict of Digital Signature Laws

Proponents of a global regulatory scheme for digital signature argue that consistent laws are needed in order to promote E-Commerce.[343] Consistent laws will facilitate flow of E-Commerce and the sale of goods and services.[344] Some commentators argue that many current digital signature laws are inconsistent with one another.[345]

Various jurisdictions have either enacted or are enacting

---

341. *See* Smith & Keehan, *supra* note 10, at 506 (describing that initial spectacular growth and accelerating use of Internet among businesses and consumers has prompted many banking industry analysts to predict widespread use of on line and Internet banking by 2000); *see also* Barassi, *supra* note 26, at 16 (explaining that E-Commerce and state of industry involved in building emerging digital authentication infrastructure are in relatively nascent state).

342. *See* Smith & Keehan, *supra* note 10, at 506-07 (stating that online banking will decrease greatly if uniform, comprehensive laws are not enacted); *see also* Tom Foremski, *Web Browsers Beat Brick and Mortar*, FIN. TIMES, Sept. 4, 1996, at 4 (showing that online banking could potentially increase from 700,000 users in 1995 to over five million users in year 2000).

343. *See* UTAH CODE ANN. § 46-3-102 (1995) (stating purpose of Utah Act is "to establish, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages"); *see also* Draft Directive, *supra* note 299, COM (1998) 297 Final, art. 3(2) (allowing Member States of European Union to introduce voluntary accreditation schemes, as long as they follow uniform rules of being "objective, transparent, proportionate, and non-discriminatory").

344. *See* Ballen & Fox, *supra* note 20, at 342 (arguing that any potential conflict between statutes addressing E-Commerce transactions must be resolved). Suppose that each jurisdiction that has digital signature statutes has a different standard for CAs and legal recognition of digital signatures. *Id.* In order for a business to take advantage of digital signatures, the business would have either to undertake operational and liability standards of acting as a CA or to rely on numerous individual CAs that are recognized in their individual jurisdiction. *Id.*

345. *See* Kiefer, *supra* note 21, at 9 (explaining that Germany and Malaysia have laws that entail significant state involvement); *see also* Barassi, *supra* note 26 (citing Spain, which has called for general methods that establish inalterability, integrity, or uniformity of signed electronic message).

digital signature schemes.[346] Digital signature legislation has been not only introduced globally, but also enacted by individual jurisdictions within a country.[347] Many U.S. states have adopted their own digital signature laws.[348] Some have followed or have used the Utah Act,[349] and some have openly rejected using the Utah Act, preferring instead to create their own legislative scheme.[350]

Some of these laws either conflict with one another or may not legally recognize digital signatures from other jurisdictions.[351] Commentators recognize both the need for consistent statutes that can fully exploit E-Commerce and the need to resolve the potential for conflict among current laws.[352] For example, members of the U.S. Congress have acknowledged that conflicting digital signature laws will have a serious negative impact on the nationwide development of electronic banking and over-

---

346. *See* Winn, *supra* note 14, at 1179 (stating that many localities, nations, and global organizations have enacted or are considering enacting laws governing use of digital signatures).

347. *See* Kiefer, *supra* note 21, at 8 (stating that more than 40 state legislatures are working on electronic authentication statutes); *see also* Hill, *supra* note 150, at 12 (stating that 30 U.S. states and District of Columbia have enacted legislation on digital signature use).

348. *See* Nora M. Jordan & Terrance J. O'Malley, *Digital Signatures and the State Law Hurdle*, 2 NO. 2 WALLSTREETLAWYER.COM: SEC.ELEC.AGE1 (July 1998) (summarizing state action on digital signature legislation).

349. *See* Minnesota Electronic Authentication Act, MINN. STAT. ANN. § 325K *et seq.* (West 1998) (setting forth Minnesota law that recognizes digital signatures in all communications); Washington Electronic Authentication Act, WASH. REV. CODE ANN. § 19.34 (West 1998) (citing Washington state law that recognizes use of digital signatures in all communications); Biddle, *supra* note 91, at 1233 (stating that Minnesota and Washington had enacted laws that closely tracked Utah Act);

350. *See* CAL. GOV'T CODE § 16.5 (West 1998) (setting forth California law that limits scope of approval of digital signatures to communications among government entities); Biddle, *supra* note 91, at 1233 (stating that California considered and rejected Utah Act as model for its law and instead enacted non-technology-specific bill designed to address transactions with government entities).

351. *See* Gesetz zur digitalen Signatur (Signaturgesetz), v. <22.7.1997> (BGBl. I S. 1870, 1872) § 15 (stating that foreign digital signatures are equivalent under act if digital signature may be checked with public signature key for which foreign certificate of another EU Member State or are from nations that are part of international agreement with Germany).

352. Ballen & Fox, *supra* note 20, at 342; *see* Jordan & O'Malley, *supra* note 348 (discussing effect of uniformity on Internet as promoting E-Commerce). The Internet can continue to attract customers because it is an established forum for commercial activity. Jordan & O'Malley, *supra*. Jordan & O'Malley opine that nationwide legal uniformity through coordination by legislators and policy makers can greatly benefit the great number of online businesses. *Id.*

all E-Commerce.[353]

Proponents of a global scheme also argue that these different state and national laws do not fully address certain subject matters and conflict with one another.[354] Some jurisdictions have enacted laws that do not fully define necessary legal parameters as they pertain to the use of a public key system.[355] Commentators are also cautious of the degree of specification among jurisdictions that have broadly defined authentication requirements with general and non-technical provisions.[356] Digital signatures from these jurisdictions may be invalid in other jurisdictions that have used specific and technical requirements.[357] Some scholars note that the differences in approaches may not derive from the differences in legal tradition or in technological preferences, but rather from the propensities of the drafters.[358]

Proponents of a global scheme fear that the biggest threat to E-Commerce is the current lack of uniformity among digital signature legislation.[359] They argue that in the current interna-

---

353. Smith & Keehan, *supra* note 10, at 509; *see* Jordan & O'Malley, *supra* note 348 (assessing effect of lack of uniformity on financial institutions). This lack of uniformity poses significant problems for financial institutions or any other entity that generates substantial online revenue through a nationwide base of customers. Jordan & O'Malley, *supra*. For example, national online brokerage firms must decide either to require paper-based signatures from all customers or to conduct business differently with customers depending on the applicable state law. *Id.* Both options entail significant costs that will probably be absorbed by all customers. *Id.*

354. *See* Barassi, *supra* note 26 (arguing that most of these laws are based on assumption that authentication infrastructure will be based on use of digital certificate-based public key cryptography)

355. *See* UTAH CODE ANN. § 46-3-305(1) (1995) (stating that subscriber identified in certificate assumes duty to exercise reasonable care to retain control of private key); *see also id.* § 46-3-103 (failing to define reasonable care).

356. *See* Barassi, *supra* note 26 (citing Spain, which has called for general methods that establish inalterability, integrity, or uniformity of signed electronic message).

357. *See* Gesetz zur digitalen Signatur (Signaturgesetz), v. <22.7.1997> (BGBl. I S. 1870, 1872) § 2(1) (defining digital signature in terms of using public key); *see also id.* § 46-3-305 (discussing control of private key).

358. *See* Barassi, *supra* note 26 (explaining that these drafters may interject their own thoughts and biases about future of digital signature development or their uses in international transactions). Malaysia and Utah have legislation that is very similar except Malaysia mandates that CAs must obtain licenses. *Id.*

359. *Id.*; *see* Jordan & O'Malley, *supra* note 348 (discussing U.S. states' progress in digital signature legislation). Jordan & O'Malley argue that while the efforts of the states are encouraging, the lack of uniformity among state statutes is a substantial obstacle to firms seeking legal certainty in servicing clients across jurisdictions. Jordan & O'Malley, *supra*. Even in states where electronically created signatures are generally acceptable for all transactions, different limitations exist on the type of signature that

tional legal environment regarding digital signatures, this lack of uniformity can create difficulties for transacting parties using digital signatures.[360] For example, a majority of jurisdictions are proposing or have created a high degree of state intervention in the public key infrastructure.[361] This state intervention may further hamper international transactions by burdening parties and the emerging legal infrastructure with inconsistent obligations.[362]

Because E-Commerce is in its nascent stages, some legal experts argue that the legal infrastructure regarding digital signatures should be consistent in order to protect it and to help it develop.[363] Some digital signature laws differ on legally acceptable definitions for a certain aspect of digital signatures.[364] For example, the Utah Act defines a digital signature as a transformation of an electronic message by an asymmetric cryptosystem.[365] The German Act has a different definition.[366] Another problem is that if a transaction uses a digital signature that does not use the private key-public key model then the transaction may not be recognized by any jurisdiction because the current laws require use of the private key-public key model.[367] The total

---

will be considered effective. *Id.* Some states allow the use of electronic signatures, while other states require digital signatures, and they do not differentiate between both terms. *Id.*

360. Barassi, *supra* note 26.

361. *See id.* (stating that state intervention may cause non-uniform legal regime by creating conflicting substantive and procedural requirements for transacting parties).

362. *See* Sabett, *supra* note 16, at 536 (stating that digital signature technology has matured significantly and that technology should be elevated to level of legal acceptability, both domestically and internationally).

363. Barassi, *supra* note 26; *see* Philip S. Corwin, *Digital Signatures and Signature Dynamics: Some Issues to Consider*, 17 NUMBER. 9 BANKING POL'Y REP. 1, 1 (1998) (arguing that E-Commerce can not thrive in vacuum and that it requires atmosphere of supportive rules). Corwin suggests that new multinational treaties and conventions can assure that global digital signature systems achieve interoperability and mutual recognition of legal rights and duties. Corwin, *supra.*

364. Smith & Keehan, *supra* note 10, at 512.

365. *Id.*; *see* UTAH CODE ANN. § 46-3-103(10) (1995) (defining digital signature as transformation of message through use of asymmetric cryptography such that recipient of message can use sender's public key to determine whether transformation was created by using sender's private key and whether message was altered since transformation was made).

366. *See* Gesetz zur digitalen Signatur (Signaturgesetz), v. <22.7.1997> (BGBl. I S. 1870, 1872) § 2(1) (defining digital signature as seal created with private key).

367. Smith & Keehan, *supra* note 10, at 512; *see* German Act, *supra* note 259, at § 2(1) (stating that digital signature is created with private key); *see also id.* § 46-3-103(10) (defining digital signature through uses of public and private keys).

effect of all these laws is that international transactions may become illegal and in the very least, the legal status of such transactions is uncertain.[368] One commentator has stated that the various legislative efforts create both an outright conflict concerning digital signature authentication and disharmony in E-Commerce.[369]

B. *Arguments Against a Global Regulatory Scheme for Digital Signatures Legal Scheme Will Promote E-Commerce*

Opponents of a global regulatory scheme for digital signatures argue that such a scheme would hamper the development and use of E-Commerce.[370] This type of scheme may impose regulations with a specific view of E-Commerce and would create market distortions if this view were not attained.[371] Some commentators also argue that an international digital signature scheme will create administrative problems and will take many years to implement fully.[372]

1. A Global Regulatory Scheme for Digital Signatures Will Hamper E-Commerce

Opponents of a global scheme argue that E-Commerce practices and standards have to come from the market.[373] They further argue that policy makers create these rules to anticipate any potential problems for digital signatures and that these policy makers may dictate a standard that may be abandoned or inefficient.[374] Opponents also argue that digital signature legis-

368. *See* Signaturgesetz, § 15 (allowing digital signature certificates from EU Member States or from nations that have treaty with Germany); *see also* Buenting, *supra* note 260, at 19 (stating that Germany has not yet signed treaty with United States regarding acknowledgement of U.S. digital signatures).

369. Barassi, *supra* note 26.

370. *See* Kiefer, *supra* note 21, at 11 (citing criticism of German Act as being inflexible and creating potential barriers for non-German companies).

371. *See* Biddle, *supra* note 91, at 1245 (arguing that time for legislation is after identifiable problems exist in mature industry and that premature regulation creates market distortions, which prevent E-Commerce from reaching its full potential).

372. *See* Juan Andres Avellan V, *John Hancock in Borderless Cyberspace: The Cross-Jurisdictional Validity of Electronic Signatures and Certificates in Recent Legislative Texts*, 38 JURIMETRICS J. 301, 310 (1998) (stating international agreements take years to draft, negotiate, and to implement by each nation involved).

373. Biddle, *supra* note 91, at 1226.

374. *See* Avellan, *supra* note 372, at 309 (arguing that current legislative approaches focus on technology of digital signatures); *see also* Biddle, *supra* note 91, at

lation cannot currently deal with liability issues and must allow the market to dictate these liability standards.[375]

a. Global Regulatory Scheme for Digital Signatures Will Improperly Anticipate Potential Problems with Digital Signatures

Opponents of current digital signature schemes argue that the emergence of E-Commerce has caused reliant interest groups to put pressure on legislatures to consider devising regulatory schemes even before it is clear whether Internet business models will be successful.[376] Opponents also note that, at this nascent stage of E-Commerce, a global regulatory scheme for digital signatures may not be able to resolve potential or unknown issues.[377] They maintain that E-Commerce has to evolve naturally according to market dictates.[378] Accordingly, they contend that any type of digital signature legislation cannot prescribe the evolution of E-Commerce because such legislation may presume an untenable vision of E-Commerce.[379] Once enacted and followed, this legislation may pose a significant risk of distorting an infant market and locking in business models that may not only harm consumers, but also hamper the future development of E-Commerce.[380] One expert has argued that refraining from legislation will permit the market to continue to develop without the distorting effects of unresponsive regulation.[381]

1228 (positing that most flaws in cryptography-related legislation are attributed to inadequate technical knowledge by the drafters).

375. *See* Biddle, *supra* note 91, at 1226 (arguing that policy makers have assumed that CA's potential liability is flaw of current laws and these policy makers use digital signature legislation to shift immense liability burden onto consumers who use public key infrastructure).

376. *See* Winn, *supra* note 14, at 1253 (stating that Clinton Administration's policy on E-Commerce is that, in absence of information showing need for regulation, legislatures should be hesitant to intervene in working of marketplace).

377. *See* Dorney, *supra* note 171, at 149 (stating that some critics think that it is too early to adopt universal technological standards for technology that is likely to evolve over time than be force to evolve through set legislative standards).

378. Biddle, *supra* note 91, at 1226.

379. *See id.* (explaining that some digital signature legislation anticipate E-Commerce to evolve according to enacted standards and not according to marketplace).

380. *Id.*

381. *See* Winn, *supra* note 14, at 1258-59 (concluding that developers and promoters of public key cryptography are seeking legislative efforts to shield them from potential liability). Sheltering developers will prevent developers from trying to improve

b. Defining a Liability Framework for Digital Signatures Can Cause Problems at This Nascent Stage

Opponents of a global regulatory scheme for digital signatures maintain that defining a liability scheme for digital signatures is not presently feasible.[382] Public key infrastructure proponents suggest that a digital signature legal framework resolves many issues surrounding liability.[383] These proponents propose that a global scheme will contain explicit liability provisions and thereby bring certainty to international E-Commerce transactions.[384] Some legal scholars counter this proposition by arguing that an open public key infrastructure implicates considerable liability risk and that this risk has to be understood before any legislation proceeds.[385] They further argue that current digital signature schemes protect CAs[386] and developers, while shifting all the risk to users.[387] Opponents of a global scheme maintain that this type of liability allocation system not only harms users in the short term, but also will harm developers in the long term.[388]

---

overall security of public key cryptography systems. *Id.* Legislators should refrain from enacting digital signature statutes in order to allow the market to continue to develop. *Id.*

382. *Id.* at 1177; *see* Biddle, *supra* note 91, at 1237-38 (arguing that currently no satisfactory solution exists for liability issues with public key infrastructure). If liability loss fell on party relying on digital signatures, then the goals of a public key infrastructure would be undermined because of great opportunity for fraudulent collusion. Biddle, *supra*, at 1237. If liability loss fell on party whose digital signature was used, then no consumer would accept this level of risk. *Id.* at 1236.

383. Winn, *supra* note 14, at 1177.

384. *See* Dorney, *supra* note 171, at 150 (stating that legal status of digital signature may be uncertain). It is possible that a digital signature would be found to be a signature, but the result is very uncertain. *Id.*

385. *See* Biddle, *supra* note 91, at 1235 (arguing that liability exposure faced by CAs with open public key infrastructure model is product of business model that can not internalize costs of fraud that may result under any public key-based system).

386. *See* UTAH CODE ANN. § 46-3-309 (1995) (limiting damages against CAs by not holding CAs liable for any loss caused by reliance on false signatures if CA complied with Utah Act). A CA does not have to pay punitive or exemplary damages, damages for lost opportunity, or pain and suffering damages. *Id.*

387. *See* Winn, *supra* note 14, at 1258-59 (describing impact of liability shifting statutes). Developers and promoters of digital signatures are seeking legislative safe harbors in order to permit them to focus solely on the work of building a public key infrastructure. *Id.* at 1258.

388. *See id.* (stating potential effect on users and developers). Less sophisticated consumers will bear potential, overwhelming losses under a liability system. *Id.* Developers are also harmed because many users will not utilize their designs. *Id.* In addition, developers may lose the incentive to improve the overall security of E-Commerce transactions. *Id.*

They contend that liability issues must be fully known and understood before they can be solved global regulatory scheme.[389]

2. A Global Regulatory Scheme for Digital Signatures Will Produce Administrative Problems in Trying to Create and to Implement the Proper Type of Digital Signature Legislation

Opponents argue that a global regulatory scheme for digital signatures will be difficult to formulate using current information.[390] They further argue that even if a global scheme were adopted, all nations involved in the scheme would take years to create legislation.[391] If a global scheme were implemented, then it might over-regulate E-Commerce and interfere in the functioning of the market.[392]

a. Global Regulatory Scheme for Digital Signatures Cannot Proscribe the Proper Type of Digital Signature Legislation in Order to Utilize E-Commerce Fully

Opponents of a global regulatory scheme for digital signatures question whether the global scheme will be one that is either technology-neutral or technology-specific.[393] Proponents of cryptography products advocate enacting technology-specific legislation because it endorses what they believe is the best solution available to the problem of authenticating users over insecure networks.[394] This type of legislation can pave the way for uniform digital signature standards.[395]

---

389. *Id.*

390. *Id.* at 1182; *see* Biddle, *supra* note 91, at 1245 (explaining that legislation is created when mature industry or market exists and digital signatures are not fully developed in their uses). Biddle suggests that digital signature laws must allow E-Commerce transactions to evolve unfettered with burdensome regulations. Biddle, *supra.* Only then can digital signatures can reach its fullest potential. *Id.*

391. Avellan, *supra* note 372, at 310; *see* Greenwood & Campbell, *supra* note 3, at 308 (explaining that some jurisdictions have laws regarding use of signatures).

392. Winn, *supra* note 14, at 1181; *see* Avellan, *supra* note 372, at 310 (positing that recognition of digital signatures by individuals governments under global scheme would turn into discriminatory practice in order to promote their domestic groups).

393. *See* Winn, *supra* note 14, at 1177 (arguing that technology-neutral approach to Internet legislation can permit parties to commercial transactions to make up their own minds about what new business practices make sense for Internet commerce).

394. *Id.* at 1181.

395. *See* Kuner, *supra* note 273 (citing goals of German Act, which is technical law

Other scholars argue that a global regulatory scheme for digital signatures should have a technology-neutral approach because this approach allows parties to commercial transactions to determine their own E-Commerce business practices.[396] Technology-neutral advocates believe that digital signature legislation should eliminate any residual disparities between the legal status of accepted business transactions and E-Commerce.[397] Any premature regulation can create market distortions that would prevent E-Commerce from coming to its fruition.[398]

One commentator notes that at this time, it is unclear what authentication, business, or technical standards will gain acceptance.[399] Also unclear is what individual users, businesses, and other parties may accept or even be expected to accept.[400] Opponents of a global regulatory scheme for digital signatures argue that legislating any sort of risk allocation scheme before any E-Commerce business practices have become established can create an unresponsive regulatory framework.[401] They argue that the time for regulation is after identifiable problems appear in a mature and ongoing industry, before an industry exists.[402]

---

that was created to provide conditions for secure infrastructure for use of digital signatures in Germany). The German government is open about its intention to create a *de facto* standard for the use of digital signatures. *Id.* The law was intended to lead to a competitive, market-driven procedure for digital signatures in Germany. *Id.*

396. Winn, *supra* note 14, at 1177.

397. *See id.* at 1181 (arguing that until full maturation of E-Commerce, no competing business model for E-Commerce security should be legislatively endorsed).

398. *See* Biddle, *supra* note 91, at 1245 (arguing that this result may be better determined by market forces rather than results envisioned by governmental policymakers).

399. Winn, *supra* note 14, at 1181; *see id.* at 1182 (stating that in absence of any concrete information about what constitutes reasonable business practices and reasonable computer security standards in this new environment, it is unclear what will constitute fair and efficient loss allocation system).

400. *See id.* at 1182-83 (citing presumption for validity of written signatures as reliable evidence of intent to be bound is grounded on well-established connection consistently observed over centuries). No basis in experience exists for extending the same, tested presumption to any electronic authentication procedure like a digital signature. *Id.*

401. *See id.* at 1183 (arguing that there is limited knowledge in area of E-Commerce). Winn argues that more knowledge is needed about how these new technologies will actually be used by the merchants and consumers that they are designed to benefit. *Id.*

402. Biddle, *supra* note 91, at 1245.

b. Restraint on E-Commerce—Problems Enacting and Implementing a Digital Signature Scheme

Opponents of global regulatory scheme for digital signatures argue that this type of law may over regulate the use of digital signatures or even create strict, unnecessary requirements.[403] They argue that these requirements can hinder E-Commerce and ultimately halt the full exploration of digital signature uses.[404] One expert has suggested that these issues arise mainly because of policy makers' lack of understanding of this technology and its potential uses.[405]

In addition to legislators' incomplete knowledge, some commentators have suggested that another factor to consider is that an international agreement on digital signatures may be impractical and ultimately become a tremendous undertaking.[406] A meeting of all concerned nations, businesses, and other interests may not reach a result that is beneficial to E-Commerce.[407] Typically, international agreements take years to negotiate, then to draft, and then finally to have legislation that must be passed by the legislatures of each party that implements the agreement.[408]

Some commentators contend that individual legislatures

---

403. *See* Kiefer, *supra* note 21, at 11 (stating that some domestic and international commentators criticize German Act for being inflexible and taking overly regulated approach). The German Act imposes stringent licensing terms on CAs by requiring users to present their identification physically to a CA in order to get a digital signature. *Id.* This stringent requirement for becoming a licensed CA can create a barrier for non-German companies acting as CAs. *Id.*

404. *See id.* at 11-12 (citing possible effects of German Act). The German Act's strict licensing terms may stop the possibility of Internet-delivered certificates because users have to be physically present with identification in order to get a digital signature. *Id.*

405. *See* Biddle, *supra* note 91, at 1228 (explaining that flaws in cryptography-related legislation could be attributed to inadequate technical knowledge by policy makers).

406. *See* Avellan, *supra* note 372, at 310 (arguing that creating international agreement would be most complex way of solving problem of ensuring that digital signatures are legally valid).

407. *See* Parker, *supra* note 24 (describing environment surrounding digital signature discussions at United Nations). When the Model Law on Electronic Commerce was ratified by the United Nations in January 1997, the United Nations Commission on Electronic Trade turned its attention to a heated debate on a model digital signature law in the closing weeks of February. *Id.*

408. *See* Avellan, *supra* note 372, at 310 (explaining that these agreements may eventually become agreements on general principles with little room for details).

may have difficulty in passing legislation implementing a global regulatory scheme for digital signatures because this international agreement may invalidate certain local and state laws.[409] Provisions in an international legal scheme could invalidate their enacted state and federal laws regarding electronic transactions.[410] These national schemes have been set up to deal with a country's specific policy concerns about E-Commerce and an international agreement would defeat a country's policy.[411]

c. A Global Regulatory Scheme for Digital Signatures Would Introduce Unnecessary Government Interference in E-Commerce

Opponents of a digital signature scheme maintain that legal issues that are raised by the increase in E-Commerce should not become a pretext for heavy-handed government intervention.[412] They argue that the explosion of digital signature legislation is because legislators fear that E-Commerce transactions and digital signatures will not be legally recognized.[413] Opponents further contend that this legislation is unnecessary because some courts have indicated that the law can be flexible and supportive

---

409. *See* Greenwood & Campbell, *supra* note 3, at 308 (stating that some states or localities can impose writing requirements). A global regulatory scheme for digital signatures may invalidate these requirements, which can range from basic contract requirements, such as a state's statute of frauds laws, to notarization and attestation issues. *Id.*

410. *See* Ballen & Fox, *supra* note 20, at 343 (explaining that United States federal government has certain federal writing requirements, most of which are intended as consumer protection measures, that require financial institutions to provide consumers with various disclosures in writing). For example, a global regulatory scheme for digital signatures may invalidate the federal Electronic Fund Transfer Act and the Federal Reserve Board's Regulation E. *Id.* Both of these measures require financial institutions that offer electronic fund transfers to their consumers to provide them with various disclosures in writing. *Id.* The writing requirement has been interpreted as requiring traditional paper writing and this requirement can not be altered by agreement. *Id.* at 343-44.

411. *See* Gesetz zur digitalen Signatur (Signaturgesetz), v. <22.7.1997> (BGBl. I S. 1870, 1872) § 1 (stating purpose of German Act is to create conditions for digital signatures under which they may be deemed secure and forgeries of digital signatures may be ascertained).

412. *See* Winn, *supra* note 14, at 1181 (arguing that current market is functioning and that no compelling evidence exists to show that competitive market forces are failing to achieve fair and efficient result).

413. *See* Biddle, *supra* note 91, at 1244 (stating that legislators have mistaken impression that special legal rules are needed to accommodate E-Commerce).

of new commercial methods, such as digital signatures.[414] Opponents also state that broad-based legislation is not needed to accommodate digital signatures, public key cryptography, or any other emerging authentication technology.[415] Business conducted through the Internet is rapidly expanding and is not yet encumbered with an intrusive, unresponsive, regulatory structure.[416] Opponents maintain that an international agreement on digital signatures might require the creation and maintenance of a complex, expensive, and even unnecessary bureaucracy.[417]

III. *A GLOBAL REGULATORY SCHEME FOR DIGITAL SIGNATURES WILL PROTECT E-COMMERCE BY ELIMINATING CONFLICTS OF LAW AND PROVIDING GUIDELINES TO PARTIES*

A global regulatory scheme for digital signatures is the best

414. *See* Hessenthalar v. Farzin, 564 A.2d 990 (Pa. Super Ct. 1989) (holding that mailgram meets requirement for signature under Pennsylvania Statute of Frauds). The Pennsylvania Superior Court emphasized that "there is no requirement in the Statute or the decisional law that a signature be in any particular form. Instead, the focus has been on whether there is some reliable indication that the person to be charged with performing under the writing intended to authenticate it." *Id.* at 993; *see* Clyburn v. Allstate, 826 F. Supp. 955 (D.S.C. 1993) (holding that since information on disk can be retrieved and printed as on paper, delivery of information on computer disk constitutes writing under insurance statute). The district court stated that "[i]n today's 'paperless' society of computer generated information, the court is not prepared, in the absence of some legislative provision or otherwise, to find that a computer floppy diskette would not constitute a 'writing' within the meaning of [statute]." *Clyburn*, 826 F. Supp at 957; *see* Benjamin Wright, *Electronic Commerce Legislation: Frequently Asked Questions*, 2 NUMBER. 2 CYBERSPACE LAW. 10 (1997) (arguing that current law is quite flexible and supportive of new methods).

415. *See Massachusetts Electronic Records and Signatures Act* § 2(b) (draft Nov. 4, 1997) (visited Jan. 15, 1999) <http://www.magnet.state.ma.us/itd/legal/mersa.htm> (on file with the *Fordham International Law Journal*) (stating purpose of Massachusetts Electronic Records and Signatures Act "is to permit and encourage continued expansion of electronic commerce and online government through operation of free market forces rather than proscriptive legislation"); *see also* Biddle, *supra* note 91, at 1244 (suggesting that broad based legislation is not needed to accommodate public key cryptography or other emerging authentication technologies). Biddle suggests that areas where current legal rules hinder E-Commerce can be addressed with narrowly targeted legislation. Biddle, *supra.*

416. Winn, *supra* note 14, at 1181.

417. *See* Dorney, *supra* note 171, at 149 (positing possible results of international agreement might require implementation of standard regulations and requirements for system of CAs). This system could be complex, costly for users, and hard to maintain for government and private industry. *Id.*

approach to protect digital signatures. A global regulatory scheme for digital signatures will eliminate the current conflicts of laws situation regarding digital signatures.[418] This scheme can also assist parties in developing uniform digital signatures.[419] The ultimate purpose of the scheme is to protect and to utilize E-Commerce fully.[420]

A. *A Global Regulatory Scheme for Digital Signatures Will Eliminate Conflicts of Law and Promote International E-Commerce Transactions*

Proponents of a global regulatory scheme for digital signatures are correct because a global scheme will protect E-Commerce from inconsistent regulations.[421] Many different levels of government have considered or proposed digital signature statutes.[422] These statutes address digital signatures from different approaches and these different approaches will hamper international E-Commerce transactions using digital signatures.[423] Although opponents of a global scheme argue that such a scheme would hinder the development of E-Commerce, they fail to take account of the present legal situation with the conflicting digital signature legislation.[424] A global regulatory scheme for digital signatures can establish consistent, uniform rules applicable to digital signatures and will promote international E-Com-

---

418. *See supra* notes 21-23 (stating that numerous nations have enacted digital signature laws and that certain U.S. states have already setup a legal framework regarding digital signatures).

419. *See supra* notes 335-37 and accompanying text (arguing that global digital signature legal scheme will facilitate E-Commerce by allowing parties to design their transactions according to enacted rules).

420. *See supra* notes 153-55 (arguing that digital signatures are catalyst to expand E-Commerce because digital signatures can authenticate identities of parties on Internet).

421. *See supra* notes 354-58 (arguing that current digital signatures laws conflict with one another).

422. *See supra* notes 167, 170-71, 256-58, and accompanying text (stating that numerous governments have enacted digital signature legislation).

423. *See supra* notes 359-62 and accompanying text (arguing that different jurisdictions have different digital signature laws and that these different laws will hamper international transactions because parties will have to comply with numerous digital signature laws imposed by their respective countries).

424. *See supra* notes 377-80 and accompanying text (arguing that digital signature legislation can not mandate evolution of E-Commerce, which must occur according to dictates of market).

merce transactions.[425]

E-Commerce transactions relate to the unfettered flow of information using a network such as the Internet.[426] Digital signatures can further facilitate E-Commerce transactions because digital signatures serve security, non-repudiation, and evidentiary functions.[427] Different schemes create hurdles for digital signature use and may slow or even block the flow of goods and services that arise from E-Commerce.[428]

B. *A Global Regulatory Scheme for Digital Signatures Will Guide Parties in Digital Signature Transactions*

A global regulatory scheme for digital signatures will provide guidance by legally recognizing certain mechanisms of digital signatures.[429] A law could permit the use of CAs and then monitor them.[430] Opponents counter that digital signature legislation cannot predict the development of digital signatures[431] and therefore cannot resolve liability issues.[432] This argument fails to recognize that a uniform, global standard is better than haphazard legislation that creates greater uncertainty in the international arena, decreases E-Commerce activities, and resolves no issues.[433] A regulatory scheme for digital signatures on a global scale will proscribe guidelines for the interaction between

---

425. *See supra* notes 338-41 and accompanying text (explaining that globally recognized standard will promote E-Commerce transactions using digital signatures by giving guidance to parties involved in E-Commerce).

426. *See supra* note 1 (defining E-Commerce).

427. *See supra* notes 106-33 (discussing security, non-repudiation, and evidentiary functions that digital signatures serve).

428. *See supra* notes 330-32 and accompanying text (arguing that parties in international E-Commerce transactions are confused in determining legal treatment of digital signatures).

429. *See supra* notes 335-37 and accompanying text (stating that global digital signature laws will legally recognize digital signature infrastructure and permit further development of this structure).

430. *See supra* notes 338-40 and accompanying text (giving example that if law recognized CAs, E-Commerce transactions involving digital signatures will be more secure because of legal recognition duties of CA).

431. *See supra* notes 379-81 and accompanying text (arguing that digital signature legislation can not dictate evolution of E-Commerce and may hinder future development of E-Commerce by requiring all E-Commerce transactions to follow legislation that may not be utilized in future).

432. *See supra* notes 385-89 and accompanying text (arguing that open public key infrastructure creates significant amounts of risk and that current legislation shifts all this risk onto users).

433. *See supra* notes 329, 351-53, and accompanying text (stating that consistent

all parties engaging in E-Commerce transactions.[434]

C. *A Global Regulatory Scheme for Digital Signatures Will Allow for Full Exploration of E-Commerce*

One of the ultimate benefits of a global regulatory scheme for digital signatures is the increase and full utilization of E-Commerce throughout all economic sectors.[435] Opponents of a global scheme argue that such a scheme would be difficult to create, to implement, and to administer.[436] This argument fails to consider the need to protect E-Commerce and digital signatures at this nascent stage with consistent laws.[437] Digital signatures can be used over the Internet in any situation where any party, from any location, wants to enter into a contract.[438]

CONCLUSION

Digital signatures can open E-Commerce and create new economic opportunities and new ways of doing business that would benefit businesses and consumers. By ensuring the security and integrity of electronic transmissions, digital signatures provide a foundation for the new age of E-Commerce. In order to apply digital signatures fully, policy makers must enact a global regulatory scheme that must set forth the legal framework for conducting E-Commerce. Policy makers must enact this legal regime on a global level in order to promote the flow of goods and services through E-Commerce and to prevent any inconsistent measures that would hinder this flow.

---

statutes can allow parties to exploit E-Commerce fully and to prevent decline in E-Commerce that can be result of current, non-consistent regime among different nations).

434. *See supra* notes 226-55 (stating Utah Act, which sets forth legal framework for all parties that use digital signatures).

435. *See supra* notes 138-43 and accompanying text (exploring possibilities and opportunities that full maturation of E-Commerce would bring).

436. *See supra* notes 393-402 and accompanying text (arguing that creating global regulatory scheme for digital signatures would be difficult because of deciding type of legislation that scheme would entail); *see also supra* notes 403-11 (describing problems of implementing potential international scheme).

437. *See supra* notes 363-69 and accompanying text (stating that E-Commerce is in initial stages and that differing standards can thwart international transactions).

438. *See supra* notes 161-66 and accompanying text (listing many uses for digital signatures as means to enter into any sensitive or non-sensitive transaction normally done on paper).