UIC John Marshall Journal of Information Technology & Privacy Law

Volume 17
Issue 3 *Journal of Computer & Information Law - Spring 1999*

Article 5

Spring 1999

Document Authentication in Electronic Commerce: The Misleading Notary Public Analog for the Digital Signature Certification Authority, 17 J. Marshall J. Computer & Info. L. 833 (1999)

John C. Anderson

Michael L. Closen

DOCUMENT AUTHENTICATION IN ELECTRONIC COMMERCE: THE MISLEADING NOTARY PUBLIC ANALOG FOR THE DIGITAL SIGNATURE CERTIFICATION AUTHORITY

by JOHN C. ANDERSON† & MICHAEL L. CLOSEN††

"I think there is a world market for maybe five computers."[1]

— Thomas Watson, Chairman of IBM, 1943.

"We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress."[2]

— Albert Gore, Vice President of the United States, 1997.

---

† Judicial Clerk, Illinois Appellate Court. Notary Public, State of Illinois. B.S., Illinois State University; J.D., The John Marshall Law School.

†† Professor of Law, The John Marshall Law School. Notary Public, State of Illinois. B.S., M.A., Bradley University; J.D., University of Illinois.

1. Margaret M. Newton, *Random Notes Redux*, 31 ARK. LAW. 6 (1996).

2. White House, *A Framework for Global Electronic Commerce*, July 1, 1997, 507 PLI/PAT, at 147, 179 (visited June 20, 1998) <http://www.iitf.nist.gov/eleccomm/ecomm.htm/>.

I. INTRODUCTION

What a difference 50 years can make! In light of advances in technology multiplying at geometric rates in less and less time, the monstrous first computers of the 1940s seem like Stonehenge era devices in comparison to today's computing achievements. What Chairman Watson did not accurately foresee, was the extent of commercial applications of the new technology. We expect that Vice-President Gore's predictions will come true—and in far less than another 50 years.

Imagine that Carroll is a diamond broker in Chicago and commonly receives phone orders to ship diamonds to Jean, a buyer in Paris. One Friday, Carroll receives an e-mail purportedly from Jean, directing Carroll to send a quantity of diamonds overnight but this time to a different address in London. It is too late to contact anyone by phone to verify this change. How can Carroll change the shipping destination while remaining confident that the e-mail came from the trusted buyer Jean?[3] Through the use of an electronic instrument digitally executed and verified by a certification authority or cybernotary.[4] Assume that a frequent gambler Pat decides to engage in on-line gaming through a Pacific Island casino corporation. How can the casino be confident that Pat is not an impostor? How can Pat be confident that any winnings will really be paid to Pat?[5] Through the use of an electronic instrument digitally executed and verified by a certification authority. If the President of the United States and the representative of a foreign government, such as the Prime Minister of Ireland, wanted to execute a diplomatic instrument almost simultaneously in separate ceremonies in their home countries without the two heads of state having to meet face-to-face, how could that process be securely accomplished?[6] By way of a digitally signed and properly verified electronic document. Goods are now being

3. Falsification of an e-mail sender's identity is a growing problem. *See generally* Hotmail Corp. v. Van Money Pie, Inc., 47 U.S.P.Q. 1020, 1998 WL 388389 (N.D. Cal. 1998) (enjoining defendants from sending "spam" e-mail messages with falsified return addresses).

4. *See* Michael L. Closen & R. Jason Richards, *Notaries Public—Lost in Cyberspace, or Key Business Professionals of the Future?*, 15 J. MARSHALL J. OF COMPUTER & INFO. L. 703, 737-41 (1997) (discussing the role of the certification authority, and identifying the nickname or synonym of "cybernotary"); James Hill, *Lock and Load: Document Security on the Internet*, BUS. LAW TODAY, Nov.-Dec. 1998, at 8 (addressing security issues in electronic commerce, including digital signatures and certification authorities).

5. *See generally* Anthony Cabot & Joseph Kelly, *Internet, Casinos and Money Laundering*, 2 J. OF MONEY LAUNDERING 134 (1998) (noting the establishment and expansion of on-line gaming).

6. Richard P. Klau, *Contract Negotiations Enter a New Dimension When Parties Can Sign On the Electronic Dotted Line*, STUDENT LAW., Nov. 1998, at 14, 16 ("In September [1998], President Clinton and Irish Prime Minister Bertie Ahern signed a U.S.-Ireland communique on e-commerce using digital signatures.").

bought and sold on the Internet; international high-stakes gaming is presently being lawfully conducted on the Internet; and the U.S. President and Irish Prime Minister have already signed a diplomatic accord on the Internet.[7] The possible applications of the technology to government and business seem endless and imperative.

The attraction of commercial trade to the Internet is likened to a modern day gold rush, as business owners and speculators clamor to stake their claims over a cyberspace territory, seeking fortunes with computerized shovels and pans.[8] Like the gold rushes of the 1800s, we have seen business-to-business Internet transactions rise from nonexistence a few years ago to $15 billion in 1998, and an expected $175 billion by 2000.[9] One cannot pick up a newspaper without reading about the Internet, or turn on a television or radio without hearing about the Internet. Whether or not we have personal access to the Internet, it has unquestionably affected virtually every facet of our economy and our lives.[10] This includes effects on business practices and legal policy.[11]

---

7. Regarding the September 1998 digital signing of the U.S.-Ireland communique on e-commerce, "It is believed to be the first time two heads of government have used the technology to sign a joint document, but it certainly won't be the last." *Id.* at 16.

8. Craig W. Harding, *Selected Issues In Electronic Commerce: New Technologies and Legal Paradigms*, 491 PLI/PAT, at 7, 9 (1997). The Internet was originally envisioned by the United States Government as a tool for communicating during a nuclear event. HARLEY HAHN, THE INTERNET COMPLETE REFERENCE 2 (1996). Eventually, the Internet evolved into a collection of tens of thousands of computer networks, stretching across the globe. *Id.* at 3. For a good general discussion of the Internet and its background, uses and characteristics, the case of A.C.L.U. v. Reno, is a good example. *See* A.C.L.U. v. Reno, 929 F. Supp. 824, 830-49 (E.D.Pa. 1996).

9. *American Software Unveils Internet Strategy: New Products To Take Advantage of $175M Market While Substantially Increasing Corporate Efficiencies*, PR NEWSWIRE, August 13, 1998, at 12:00:00. The Internet has experienced extraordinary growth, increasing from less than 300 computers in 1981 to nearly 10,000,000 host computers (sixty percent or which are in the United States) in 1996, not including the personal computers used to access the Internet. *See* A.C.L.U. v. Reno, 929 F. Supp. at 830. By 1999, an estimated 200 million people will have regular access to the Internet. *Id.* Of course, estimates do vary somewhat. Another report said "busines-to-business purchases [online], such as the wholesale purchase of supplies, could reach $300 billion by 2002 . . . .". *Internet Traffic Booming*, DAILY SOUTHTOWN [AP], April 4, 1998, at 1.

10. During the 1998 World Cup soccer competition, computer manufacturer Hewlett-Packard supported the games by maintaining an official Web site, providing scores and other information. *See Sponsors Going For Gold Rivals Vie to Replace IBM in Olympics*, THE ARIZ. REPUBLIC, August 8, 1998, at C11, *available in* 1998 WL 7789577. The site received over 1.5 billion visits in a mere five weeks. *Id.*

11. "We expect rapid, fundamental shifts in commerce as digital technology sweeps the globe." Richard D. Marks, *Subject: Information Technology*, A.B.A. J., Feb. 1999, at 36; *see also* BUS. WIRE, Sept. 16, 1998, 13:05:00 (discussing the liberalization of the U.S. government's policy on exporting encryption technology); *Internet Policies Not Disclosed*, NEWSDAY, June 4, 1998, at A55, *available in* 1998 WL 2672555 (stating that many companies on the Internet are not following the U.S. government's privacy guidelines, and such avoid-

Small businesses that use the Internet commonly have average revenues of over a million dollars more than those that do not.[12] The Internet not only increases potential small business revenues, but it also supplies a shot in the arm to large businesses and the economy as a whole.[13] One study indicates that the Internet will provide a boost to the economy of $124 billion this year, and over half a trillion dollars in 2002.[14] By 2002, American businesses will spend more than $200 billion dollars on Internet-technology deployment, or one-fifth of America's total spending on technology.[15] The establishment of the first fully on-line law school has even recently been announced.[16] Realistically, it is impossible to determine the future of the Internet and its impact at any given moment.[17] One thing is abundantly clear—that the Internet's profit potential has indeed started the gold rush of our time. Unfortunately, there also exists modern day claim jumpers, cheats and bandits, and they are very good at what they do.

A novel but serious illustration of the vulnerability of the security of electronic communications occurred in October of 1998, when millions of America Online ("AOL") e-mail messages were disrupted by an impostor

---

ance may prompt congressional action); Alan Pearce, *Regulating the Net*, AM. NETWORK, Mar. 15, 1998, at 14, *available in* 1998 WL 15870849 (discussing political and policy issues regarding enhanced applications of the Internet); Walter Hamilton & Thomas S. Mulligan, *SEC Cracks Down on Internet Stock Fraud Securities: Agency Brings Charges Against 44 People and Companies*, L.A. TIMES, Oct. 29, 1998, at C1, *available in* 1998 WL 18887991 (discussing the pervasive problem of illegally promoting stocks over the Internet).

12. *Key Facts On the Internet*, THE PATRIOT LEDGER, August 1, 1998, at 22, *available in* 1998 WL 8096129. Of the small businesses with Internet access, the average revenue is $3.79 million, compared to $2.72 million for those not using the Internet. *Id.*

13. Computer supplier Dell takes in $4 million dollars per day from its Internet transactions. *See BT: Companies Under Utilizing [sic] Technology*, M2 PRESSWIRE, August 10, 1998, *available in* 1998 WL 16516785.

14. Olson, S., *Mining the Online Economy: Electronic Commerce Software*, VOLPE WELTY & CO., January 10, 1997, at 3.

15. *Id.*

16. *See* William M. Bulkeley, *Kaplan Plans A Law School Via the Web*, WALL ST. J., Sept. 16, 1998, at B1, *available in* 1998 WL-WSJ 18984587 (describing Kaplan Education Center's plan to form Concord University School of Law, offering on-line classes in December of 1998); *Kaplan Opens On-Line: Only Law School Based in L.A.*, L.A. TIMES, Sept. 16, 1998, at D2, *available in* 1998 WL 18874435. Graduate law degrees are also being introduced over the Internet. *See First On-line Degree Approved by the ABA*, NAT'L JURIST, Oct. 1998, at 12 (reporting the approval of an on-line LL.M. degree in International Taxation, at Regent University School of Law); David Rubiales, *Distance Learning and the Virtual Classroom: Faculty Learns New Tricks*, FOOTNOTES [AAUP], Fall 1998, at 7 ("The past decade has witnessed the widespread development of distance learning courses . . . whether offered via television or online . . . .").

17. A.C.L.U. v. Reno, 929 F. Supp. at 831. Not only is it impossible for a single person to completely understand the Internet as a whole, but it is impossible for a single person to understand most of it. Hill, *supra* note 4, at 2.

who forged an electronic document.[18] The impostor succeeded in directing the company, which maintains the electronic address book for AOL and many other Internet entities, to change AOL's internet address.[19] Apparently, AOL simply had not employed a sufficient level of security to protect against this impostor's vandalism.[20] The disruption lasted for more than six hours and affected some 4-5 million e-mail messages.[21] This security breach was especially troublesome in light of the fact that AOL "controls by far the largest pool of online consumers" and, therefore, occupies the "position [of] dominant Internet gateway for consumers."[22] The WALL STREET JOURNAL correctly observed that this "incident served as a dramatic new reminder of security risks online."[23]

The Federal Bureau of Investigation ("FBI") estimates that the Internet is involved in some eighty percent of all computer crime.[24] The authors predict that percentage will grow dramatically. Considering the widespread and escalating use of the Internet and the transactions it handles that is scary news. As one possible example, ask whether drug dealers and other racketeers might seek to launder the large sums of money they acquire (usually in small denominations) through gaming with on-line casinos.[25] Gaming observers have recently predicted: "Money laundering, casinos and the Internet may become unavoidably intertwined in the next decade."[26] The extensive Native American gaming enterprises in the United States may be drawn into this mix.[27] As

18. *See* Thomas E. Weber, *E-Mail Sent to AOL Users Victim to Attack on Internet's Address Book*, WALL ST. J., Oct. 19, 1998, at B10 (detailing the October 16, 1998, disruption of millions of AOL messages for several hours); *see* Sara Nathan, *AOL Computer Service Fixes Problem After Forged Message Tangles E-mail*, USA TODAY, Oct. 19, 1998, at 7A (reporting that the AOL disruption lasted over six hours and affected between 4.2 and 5.2 million messages).

19. Weber, *supra* note 18, at B10.

20. Nathan, *supra* note 18, at 7A.

21. *Id.*

22. Thomas E. Weber, *AOL Net Soars to $68 Million; Beats Forecasts*, WALL ST. J., Oct. 28, 1998, at A3.

23. Weber, *supra* note 18, at B10. The authors would hasten to observe that we doubt the incident will have much of a financial effect on AOL since it recorded a highly successful tripling of the company's net income for the first fiscal quarter ending September 30, 1998, over the same 1997 period—from $19.2 million in the first quarter of 1997 to $68 million in the first quarter of 1998. *See* Weber, *supra* note 22, at A3. We suspect that AOL officials were eager to release this data soon after the security breach episode. That incident occurred on October 16, 1998. *See* Weber, *supra* note 18, at B10. The first quarter financial data was released on October 27, 1998. *See* Weber, *supra* note 22, at A7.

24. DAVID ICOVE, ET AL., COMPUTER CRIME: A CRIMEFIGHTER'S HANDBOOK 129 (1995).

25. *See generally* Cabot & Kelly, *supra* note 5, at 134 (discussing the ways in which money can be laundered through on-line gaming).

26. *Id.* at 134.

27. *Id.* at 138-39. "Native American gambling interests have also indicated interest in establishing Internet gambling." *Id.* at 139.

another possible example, if a thief were able to break into a bank's computer system and steal $1 million, actual total losses could readily exceed $100 million due to network downtime, application of expensive auditing procedures, and insurance premium increases, not to mention losses resulting from negative publicity and fleeing depositors.[28] Incidents of Internet fraud are no longer isolated, and many companies are taking steps to try to avoid such situations.[29] A survey conducted on behalf of the FBI estimated computer security losses of $100 million in 1996.[30] Internet fraud has become such a problem that the United States Senate Subcommittee on Investigations held hearings on the matter.[31] An expected conclusion to be drawn from those hearings was that "[a]s the Internet emerges as an important medium of commerce, it poses new risks . . . of fraud."[32] Among the many Internet security issues facing lawmakers, a partial solution that has come to the forefront is the use of digital signatures to authenticate documents.[33]

Described in more detail later, digital signatures that are verified by certification authorities through a system of key pair encryption technology provide a means for the recipients of electronic documents to verify the senders' identity and to confirm that the documents have not been altered.[34] Simply stated, a digital signature is a unique combination of letters and numbers generated by a mathematical algorithm, used to en-

28. *VeriSign Introduces Digital Certificate Solution to Secure Enterprise Servers: Organizations Benefit from Centralized Issuance and Control with VeriSign OnSite for Secure Server IDs*, PR NEWSWIRE, June 3, 1998, 08:21:00.

29. Reports of Internet fraud tripled between 1996 and 1997. David Hayes, *Internet Fraud: Oh, What A Tangled Web! The Number of Complaints About Computer Crooks Is Rising Sharply*, YORK DAILY REC., Mar. 2, 1998, at D6, *available in* 1998 WL 6211361. Last year, companies spent roughly $6.3 billion on computer network security systems, a figure that is expected to double by 2000. *See* L.A. Lorek, *Security the Focus for Businesses as Internet Crime Increases*, FT. WORTH STAR-TELEGRAM, Oct. 20, 1997, at 23, *available in* 1997 WL 11913906.

30. Lorek, *supra* note 29, at 23. The FBI estimates that less than fifty percent of all computer system break-ins are reported. *Id.*

31. Susan Collins, *Senate Subcommittee To Hold Hearings On Fraud On the Internet*, GOV'T PRESS RELEASES, Feb. 4, 1998, *available in* 1998 WL 7321509.

32. *Id. See also* Hill, *supra* note 4, at 8 (observing that "as the amount of electronic commerce increases over the next few years, the amount of fraud is likely to escalate unless security measures keep pace"). In a situation more apt for a movie, hackers broke into the Internet site Yahoo, demanding release of an imprisoned computer hacker and threatening to unleash a devastating virus on December 25, 1998. Yahoo's hacked Web site read "The virus can be stopped. But not by mortals." *Hackers Leave Ransom Note on Yahoo Site*, L.A. TIMES, Dec. 10, 1997, at D2, *available in* 1997 WL 14008548.

33. *See* Hill, *supra* note 4, at 10 (opining that "[d]igital signatures have proven secure after more than a decade of scientific review . . . .").

34. *Everything You Always Wanted to Know About Digital Signatures*, AUSTL. BUS. INTELLIGENCE, Dec. 1, 1997, *available in* 1997 WL 18182378.

crypt an electronic document through the use of a "private key."[35] A certification authority establishes a repository of clients and issues both public keys and unique private keys to each.[36] A certification authority can then determine that an electronic document has been sent by a client-sender (rather than having been sent by an impostor) and that the electronic message is genuine (rather than having been tampered with), and then can issue a certificate to such effect.[37] The certification authority also assures transmittal of the document to the true client-recipient.[38] Using the same process, a responsive message can be sent.

Because one of the certification authority's principle duties is to identify a document's singer, many commentators have, perhaps improperly, nicknamed the certification authority as a "cybernotary."[39] Indeed, oversight of the "cybernotary" is even statutorily reposed in the same state agencies that oversee the office of notary public.[40] However, this comparison to the similar but distinctly separate office of the notary public may be misplaced.

This essay addresses the use of digital signature technology and the certification authority, and poses the fundamental question of whether the traditional notary public should really serve as the model for the new position of certification authority. This paper begins with an historical review of the concern about document security and the measures taken to deal with those concerns. Second, the paper includes a very brief overview of the technological aspects of the digital signature and its value in the global marketplace. Next, this essay examines the similarities between the traditional notary and the certification authority, including the functions and responsibilities of each. We will also review the sub-

35. MARCUS GONCALVES, FIREWALLS COMPLETE 611 (1998). A "private key" is one that "belongs to a principal and is never revealed to anyone . . . and is used to encrypt a message digest [or hash function] sent by the principal to anyone else." *Id.*

36. *See* UTAH CODE ANN. § 46-3-201 (Supp. 1997).

37. *See* Closen & Richards, *supra* note 4, at 732-738 (discussing the electronic document security process). "The hope and expectation is that computer technology will improve and even assure the security of on-line transactions." *Id.* at 732. "[A] digital signature transmission that uses the cryptographic methodology is considered 'some of the most secure communication possible'." *Id.* at 738.

38. *See* Closen & Richards, *supra* note 4, at 734-737 (explaining the process of matching the sender and recipient in the electronic verification process).

39. *See, e.g.*, Closen & Richards, *supra* note 4, at 704-714 (referring to "cybernotarizations" and "cybernotaries"); Closen & Richards, *infra* note 195, at A19 (referring to "cybernotaries").

40. *See* Closen & Richards, *supra* note 4, at 719 (noting that the state agency that oversees and regulates notaries is typically the secretary of state's office). In Florida, the Executive Office of the Governor is the agency to oversee both notaries and certification authorities. *See also* Legislative Review, NOTARY BULL., Feb. 1999, at 6 (pointing out legislation in Colorado provides for appointment of notaries by the Secretary of State and "permits Secretary of State to develop rules for digital signatures").

stantial differences between the two and the potential problems that may be caused in part by assuming the notary public and certification authority have an analogous relationship. Then, the essay suggests that lawmakers more carefully guard the office of certification authority to ensure it is held as a position of respect to help assure cybernotarized documents will be accepted both domestically and internationally. This essay concludes that certification authorities should hold a distinct, vital, and respected position, with a heightened duty of care owed to subscribers to adequately ensure the continued growth of secure electronic commerce.

II. HISTORICAL BACKGROUND

Historically, the possibilities that memories would fail or parties would die, that fraud would be perpetrated, and that evidence would be lost encouraged parties to take steps to document transactions in an attempt to establish their genuineness. Since the earliest days of written language and recorded history, efforts to authenticate transactions have been undertaken, with varying degrees of success. The ancient Chinese, Greeks, and Romans reduced transactions to written form, and the use of secret codes were first employed to heighten the security of communications by at least the Third Century B.C.[41] "The ancient Assyrians and Chinese utilized the first recorded fingerprints in conjunction with the signing of legal documents . . . ."[42] The Babylonians placed documents in writing on clay tablets and impressed their fingerprints into the clay as a way of verifying those writings.[43] Illiteracy was so pervasive that documents were often authenticated with seals rather than signatures.[44] Documents—particularly multiple-page instruments—were bound together with ribbon or cord over which molten wax was poured and into which a seal from a signet ring or stamp of a family coat of arms was

41. *See* Hill, *supra* note 4, at 8 ("The use of secret codes for safeguarding important information dates back at least to the third century B.C. during the reign of Alexander the Great."). The question of what constitutes a writing for document integrity purposes continues to be an issue as various kinds of modern technologies create their own unique forms of documents. *See, e.g.*, McMillan Ltd. v. Warrior Industries, 512 So. 2d 14 (Ala. 1986) (mailgram as a writing); Bazak Int'l Corp. v. Mast Industries, Inc., 73 N.Y.2d 113, 7 U.C.C. Rep.2d 1380 (N.Y. 1989) (fax as a writing); Joseph Denunzio Fruit Co. v. Crane, 79 F. Supp. 117 (S.D. Cal. 1948) (telex as a writing); Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212 (D. Colo. 1972) (tape recording as a writing). *But see* Roos v. Aloi, 487 N.Y.S.2d 637 (Sup. Ct. 1985) (holding that a tape recording is not a writing); Georgia Dept. of Transportation v. Norris, 474 S.E.2d 216 (Ga. Ct. App. 1996) (holding that a fax is not a writing).

42. Vincent J. Gnoffo, *Requiring A Thumbprint for Notarized Transactions: The Battle Against Document Fraud*, 31 J. MARSHALL L. REV. 803, 806 (1998).

43. *Id.*

44. RESTATEMENT (SECOND) OF CONTRACTS § 94, Topic 3 (1981).

impressed for identification and authentication purposes.[45] If the seal was disturbed, the possibility of tampering was evident.[46] The English Parliament in 1677 enacted the Statute of Frauds, which mandated that certain kinds of contracts must be supported by written evidence in order to obtain legal enforcement.[47] Beginning in very early times, parties to written instruments have often employed the services of witnesses to attest to the identity of document signers and to the validity of their signatures.[48] In modern times, some document signing ceremonies have been filmed or videotaped as an additional security measure.[49] We are presently in the early stage of development of various forms of biometric verification of the identity of parties to transactions.[50]

---

45. Michael L. Closen & G. Grant Dixon, *Notaries Public from the Time of the Roman Empire to the United States Today and Tomorrow*, 68 N.D. L. REV. 873, 875 & n.15 (1992); *CLE Liaison Committee*, NOTARIES PUBLIC: A HISTORY AND UNOFFICIAL GUIDE, 43 R.I. B.J., Nov. 1994, at 13; Closen & Richards, *supra* note 4, at 714 n.66. *See also* Hill, *supra* note 4, at 10 (pointing out that while the Statute of Frauds requires a signature, it "does not, however, consider a transaction invalid without a signature, but merely unenforceable in court.").

46. RAYMOND C. ROTHMAN, NOTARY PUBLIC PRACTICES AND GLOSSARY 1 (1978).

47. The original Statute of Frauds was "[a]n act for the prevention of frauds and perjuries." 29 Car. II c. 3 (1677).

48. Of course, this practice has been incorporated into, and made mandatory by, a wide variety of statutes. For example, in the estate planning field, statutes regularly require witnesses to wills, living wills, and/or powers of attorney. *See also* Record Witnesses in Journal Entry, NOTARY BULL., Feb. 1999, at 15.

> A variety of circumstances may require witnesses . . . the mark of an illiterate or disabled signer typically requires the presence of two witnesses in addition to the Notary. Recordable real estate documents in many states require the signature of one or two witnesses to the document's execution, in addition to the Notary.

Id.

49. *See* Emily Berendt & Laura Lynn Michaels, *Your HIV Positive Client: Easing The Burden On The Family Through Estate Planning*, 24 J. MARSHALL. L. REV. 509, 519 (1991) (advising that the execution ceremony of a will be videotaped under certain circumstances). However, the use of video is not always appropriate or legitimate. *See* Kevin Johnson & Gary Fields, *Jewell Investigation Unmasks FBI 'Tricks,'* USA TODAY, Nov. 8, 1996, at 13A, *available in* 1996 WL 2075026 (stating that the FBI attempted to trick Olympic bombing suspect Richard Jewel into signing a document that waived his rights to an attorney. FBI agents reportedly asked Jewel to sign the document in order to make his videotaped interrogation "appear more authentic"). Moreover, because videotaping can be very revealing, it could actually unmask the incompetence of a document signer or diminish the signer's credibility. In the recent case of President Clinton's testimony to the Starr grand jury, some observers concluded that it was a strategic mistake to videotape the testimony because it eroded the President's image and credibility.

50. Such forms might include "fingerprints, hand geometry, retina scans, and signature or voice verification." David A. Petti, *An Argument for the Implimentation of a Biometric Authentication System ("BAS")*, 80 J. PAT. & TRADEMARK OFF. SOC'Y 703, 703 (1998). "[W]idespread regulation of biometrics remains uncharted territory in the legal framework of the United States." *Id.*

Technology has advanced the speed with which documents can be created and transmitted. As parties execute and rely upon such documents, the law, in turn, has had to contend with and determine the level of trust to be placed in the technology and the resulting documents. Early legal cases, for example, followed the invention and widespread use of the telegram, telex, and mailgram.[51] The first cases concerning each of those commercial transactions dealt with various facets of their trustworthiness.[52] Later, the law confronted issues of document reliability regarding instruments created by carbon paper copying, mimeograph machines, and photocopiers.[53] More recently, documents have been created, stored, and printed out through the use of computers.[54] Also, documents are often copied and transmitted by facsimile machines, and legal cases have only begun to address the issues concerning the meaning and effect to be accorded faxed documents.[55]

---

51. *See, e.g.*, Howley v. Whipple, 48 N.H. 487 (1869) (finding that a contract made via telegraph satisfied the Statute of Frauds). Indeed, even modern cases occasionally steal deal with the basic question of reliability of technological developments invented long ago. *See, e.g.*, Hillstrom v. Gosnay, 614 P.2d 466 (Mont. 1989) (finding a contract was evidenced by a telegram).

52. *See, e.g.*, Matteson v. Noyes, 25 Ill. 591 (1861) (applying the best evidence rule to telegrams); Joseph Denunzio Fruit Co. v. Crane, 70 F. Supp. 117 (S.D. Cal. 1948) (addressing whether a telex is a writing); Franklin County Coop v. MFC Services, 441 So.2d 1376 (Miss. 1983) (discussing telex as a signature); Hideca Petroleum Corp. v. Tampimac Oil Int'l Ltd., 740 S.W.2d 838 (Tex. Ct. App. 1987) (same); McMillan Ltd. V. Warrior Drilling & Eng. Co., 512 So.2d 14 (Ala. 1986) (addressing a mailgram signature); Hesenthaler v. Farzin, 388 Pa. Super. 37 (1989).

53. Nowhere is it mandated that there can be only one "original" of a document or that only one "original" can have evidentiary weight and can be admissible. There may be multiple originals, and copies of documents may be accurate and admissible as evidence, including documents stored in computers. *See* FED R. EVID. 1002 (Requirement of Original) ("To prove the content of a writing, recording or photograph, the original writing, recording or photograph is required, except as otherwise provided by these rules or by Act of Congress." (emphasis added)). RULE 1004 (Admissibility of Evidence of Contents) proceeds to set out several circumstances under which the original is not required. RULE 1003 (Admissibility of Duplicates) provides that duplicate are admissible to the same extent as an original unless: (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." RULE 1003; *See also* FED. R. EVID. 1001(4).

54. *See e.g.*, FED. R. EVID. 1001(4) ("A 'duplicate' is a counterpart produced by the same impression as the original or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent technique which accurately reproduces the original."); People v. Avila, 770 P.2d 1330 (Colo. Ct. App. 1988) (material on a computer disk is a writing); Clyburn v. Allstate, 826 F. Supp. 955 (D.S.C. 1993) (computer printout is a writing); People v. Rushton, 626 N.E.2d 1378 (Ill. App. Ct. 1993) (computer printout is a writing).

55. *See, e.g.*, Parma Tile Mosaic & Marble Co., Inc. v. Est. of Short, 663 N.E.2d 633, 635 (N.Y. 1996) (rejecting the contention that a fax machine's automatic imprinting of the sender's name on each page satisfied the Statute of Frauds' signature requirement); Mad-

In every instance to date, technology has handily outpaced both statutory and common law in establishing the foundational and experiential bases for determining document reliability. And in each instance cited above, by the time reported legal decisions were published the courts had placed their imprimaturs of trust upon the technology, which was by then no longer novel and which had become commonly accepted by business people of integrity.[56] This has been the natural pattern of past developments. Law has been relegated to a reactionary position, unable and unwilling to lead the parade of technology.[57] However, as we shall posit later, the arrival and expansion of digital signature technology may be the first occasion for technology and statutory law to move forward virtually hand-in-hand.[58]

Of course, the additional historic measure taken to instill greater trust in written documents has been the act of notarization.[59] Since ancient times, governments have tended to create and empower the post of notary public (or its foreign equivalent).[60] These impartial public officials have been charged with the responsibility of identifying document signers, and in certain circumstances of also administering oaths to document signers.[61] Importantly, the functions of notaries public have been performed in face-to-face settings with document signers and have been

---

den v. Hegadon, 565 A.2d 725 (N.J. Super. 1989) (discussing a faxed signature); Bogue v. Sizemore, 608 N.E.2d 1246 (Ill. App. Ct 1993) (addressing the faxed acceptance of a contract offer); *But see* Georgia Dept. of Transportation v. Norris, 474 S.E.2d 216 (Ga. Ct. App. 1996) (holding that a fax does not constitute a writing).

56. A problem with electronic commerce may become the rapid pace at which it is catching on, in comparison to the slower process by which earlier technological developments were adopted. "The Internet is growing faster than all other technologies that have preceded it. Radio existed for thirty-eight years before it had 50 million listeners, and television took thireteen years to reach that mark. The Internet has crossed the line in just four years." *Internet Traffic Booming*, DAILY SOUTHTOWN [AP], April 16, 1998, at 1-2.

57. *See generally* Gregory E. Perry & Cherie Ballard, *A Chip By Any Other Name Would Still Be a Potato: The Failure of Law and Its Definitions To Keep Pace With Computer Technology*, 24 TEX. TECH. L. REV. 797 (1993).

58. Tod Newcombe, *Congress, States Struggle Over Destiny of Digital Signatures*, 44 (July 1998), <http://govt-tech.govtech.net/gtmag/1998/july/electroniccommerce/electroniccommerce.shtm>. There is no time to lose, however, in the effort to keep the legislation on digital signature security contemporaneous with technological and other legislative advances. "We also know governments and laws are not keeping pace with technological change." Marks, *supra* note 11, at 36.

59. Closen & Dixon, *supra* note 45, at 874-78. But the number of notaries public in this country has grown so dramatically that we had about 4.5 million of them at one time ("a preposterous overabundance,") and they have lost much of the historic respect reposed in their noble office. Michael L. Closen, *Why Notaries Get Little Respect*, NAT'L L.J., Oct. 9, 1995, at A23.

60. Closen & Dixon, *supra* note 45, at 882-84.

61. *See* Michael L. Closen, *The Public Official Role of the Notary*, 31 J. MARSHALL L. REV. 651, 660-61 (1998).

conducted within the territorial boundaries of the governmental entities that commissioned or licensed the notaries (which were sometimes counties or parishes).[62] Many public and private agencies require the services of a traditional notary public to witness signatures on documents as a security measure.[63] "[T]o achieve this level of genuine trust of the authenticity of a document, the usual procedure has been that the document be signed by one or more parties, that the identity of each signer be confirmed by the notary, and that the notary memorialize the transaction . . . ."[64]

An important feature of this memorialization of the notarization has included the attachment of a certificate of notarization, including signing by the notary and affixing of the notary seal.[65] Since notaries must be individual people, they have had to sign their handwritten formal signatures.[66] Notary seals have developed and changed along with technol-

62. Closen & Richards, *supra* note 4, at 724 & n.129, *citing* CAL. GOV'T CODE §§ 8200-8230 (West 1992); COLO. REV. STAT. §§ 12-55-101 to 123 and 12-55-201 to 211 (West 1996); IDAHO CODE §§ 51-101 to 123 (1994); N.M. STAT. ANN. §§ 14-12-1 to 20 (Michie 1995); N.Y. EXEC. LAW §§ 6-130 to 139 (McKinney 1993); 57 PA. CONS. STAT. ANN. §§ 1 to 169 (West 1996); VT. STAT. ANN. tit. 24 §§ 441-446 (1992); WYO. STAT. §§ 32-1-101 to 113 (Michie 1996). All states have some form of requirement that the notary reside within the state, or if the notary resides in a contiguous state s/he must conduct business within the forum state. *See, e.g.*, Cal. Gov't Code § 8201(a) (West 1992) (residency required); D.C. CODE ANN. § 1-801(a) (1992) (residency required or sole place of business); IOWA CODE ANN. § 77A.3 (West 1992) (residency required or bordering state resident and business); N.M. STAT. ANN. § 14-12-2(a) (Michie 1995) (residency required). A notary does not have jurisdiction outside the state of his/her appointment, however. *See, e.g.*, Garza v. Serrato, 699 S.W.2d 275 (Tex. Ct. App. 1985) (denying shorthand reporter for the State of Texas the authority to administer oaths in Mexico). Notaries in Alabama and Kentucky may have only countywide authority, and in Louisiana they have authority only in their parishes (unless they are also attorneys, in which case they get statewide authority).

63. MICHAEL L. CLOSEN, ET. AL., NOTARY LAW & PRACTICE: CASES & MATERIALS 115 (1997) [hereinafter NOTARY LAW & PRACTICE]. A notary public is:

> A public officer whose function is to administer oaths; to attest and certify; by his hand and official seal, certain classes of documents, in order to give them credit and authenticity in foreign jurisdictions; to take acknowledgments of deeds and other conveyances, and certify the same; and to perform certain official acts, chiefly in commercial matters . . . .

BLACK'S LAW DICTIONARY 1060 (6th ed. 1990).

64. NOTARY LAW & PRACTICE, *supra* note 63, at 10-11.

65. *See generally* Karla J. Elliott, *The Notarial Seal—The Last Vestige of Notaries Past*, 31 J. MARSHALL L. REV. 903 (1998) (discussing the importance of the affixation of a notary seal); *See also* Closen & Dixon, *supra* note 45, at 884-885.

66. *See, e.g.* ARK STAT. ANN. § 21-14-107(a) ("[A]t the time of notarization, the notary public shall sign his official signature on every notary certificate."); CAL. GOV'T CODE § 8206(a)(2) ("The certificate [of notarization] shall be signed by the notary public in the notary public's own handwriting."); COLO. REV. STAT. ANN. § 12-55-112(1) ("At the time of notarization, a notary public shall sign his official signature on every notary acknowledgment."). This procedure is in contrast to the system in which certification authorities are likely to be law firms, banks, mortgage companies, real estate agencies, and other corpo-

ogy—first there were waxen seals,[67] then there were metal embossers,[68] and now there are rubber inkstamp seals.[69] The presence of the notarial seal lends an air of ceremony, seriousness, and credibility to an instrument,[70] although the presence of a notary seal does not guarantee against either fraud in an instrument or fraud in the notarial process.[71]

Notaries in several states are required to maintain a bond, and a sequential chronological record, or a journal of their notarizations.[72] In one state, California, a notarial journal entry for certain real estate documents must include the document signer's right thumbprint.[73] Some kinds of documents have even been developed solely for the purpose of adding security to other kinds of written instruments and transactions. As examples, consider the signature guarantee commonly used in banking and other financial institutions,[74] and the notarial practice of copy

---

rate/business entities, rather than individual persons. *See also* Closen & Richards, *supra* note 4, at 739 ("[A]lthough notaries must be human beings, certification authorities or cybernotaries can be entities such as accounting firms, banks, real estate enterprises, and the like.").

67. Elliott, *supra* note 65, at 907.

68. *Id.* at 907.

69. *Id.* at 907.

70. Douglass M. Fischer, *The Seal: Symbol of Security*, NAT'L NOTARY MAG., Nov. 1995, at 10.

71. See the numerous cases of fraud, including notarial collusion, reviewed in NOTARY LAW AND PRACTICE, *supra* note 43, at 247-277, 288-289, 301-310; Closen & Dixon, *supra* note 45, at 892; Closen, *supra* note 61, at 676; Vincent Gnoffo, Comment, *Notary Law and Practice for the 21st Century: Suggested Modifications for the Model Notary Act*, 30 J. MARSHALL L. REV. 1063, 1086-87 (1997).

72. Peter J. Van Alstyne, *The Notary's Duty To Meticulously Maintain a Notary Journal*, 31 J. MARSHALL L. REV. 777, 778 & n.5. States requiring notaries to maintain a journal include Alabama, Arizona, California, Colorado, Hawaii, Maryland, Mississippi, Missouri, Nevada, Oklahoma, Oregon, Pennsylvania, Tennessee, Texas and the District of Columbia. In contrast, Kentucky, Louisiana, North Dakota and Ohio only require notaries to journalize notarial protests. Journalization is merely recommended in Alaska, Connecticut, Florida, Idaho, Maine, Massachusetts, Michigan, Nebraska, New Hampshire, New Mexico, South Dakota, Utah, Vermont and Wisconsin. *Id.*

73. Gnoffo, *supra* note 42, at 805 & n.19 (CAL. GOV'T CODE § 8206(a)(7) (West 1992 & Supp. 1996)).

74. "Signature guarantees are not notarial acts, and anyone performing a signature guarantee must not use the title and seal of a Notary Public when doing so. Signature guarantees are used by banks and other financial institutions, to authenticate signatures on documents related to the transfer of securities. The signature on the document is visually compared with another kept on file." NAT'L NOTARY ASS'N., 101 USEFUL NOTARY TIPS, at 40 (1995). *See also Signature Guarantees & Notarizations: They're Like Apples and Oranges*, THE NOTARY, Sept.-Oct. 1998, at 4 ("The difference [between a notarization and a signature guarantee] is that the notary does not 'guarantee' the signature is not a forgery. The signature guarantee does in fact make such a guarantee. The financial institution stands behind the guarantee and is liable if [it] is wrong.").

certification permitted by statutes in some states.[75] The notarial log or journal whose entries support a document's notarization also illustrates this point.[76]

In the earliest days, this notarial process worked particularly well, for notaries were few in number and could nearly guarantee the identities of document signers because people simply knew one another in these face-to-face encounters within their limited geographical territories.[77] As the population grew and as the number and jurisdiction of notaries grew (to statewide areas), the level of document security provided by the act of notarization became less predictable.[78] Simultaneously, the volume of transaction activity grew. Notaries are now regularly confronted face-to-face by total strangers bearing a variety of documents of identification, all of which are subject to alteration and forgery.[79] These crooks can be very skillful at forging documents of identification and forging signatures.[80] And, more impostors go undetected.

---

75. *See* NOTARY LAW AND PRACTICE, *supra* note 63, at 195-199 (explaining the authority of notaries in some states to perform copy certifications). *See, e.g.*, CAL. GOV'T CODE § 8205(a)(4); COLO. REV. STAT. ANN § 12-55-110(1)(c).

76. Van Alstyne, *supra* note 72, at 779-782 (discussing the evidentiary value of a notarial journal).

77. Closen & Richards, *supra* note 4, at 718-719.

78. This decline is attributable to several factors including the lack of knowledge and concern by notaries about their duties, the significant growth in the number of notaries, the minimal qualifications required of them, and the increase in breaches of ethics by notaries. *See* Closen, *supra* note 59, at A23. Of particular concern is that public and private entities require far too many documents to be notarized. *Id.*

79. *See* Nat'l Notary Ass'n, *Spot Those Imposters*, NAT'L NOTARY, Jan. 1999, at 27 ("All identification documents should be carefully inspected for evidence of imposture, alteration and counterfeiting. There is no absolute and foolproof method to detect every false ID . . . ."); Maudlyne Ihejirika, *Latinos Blast Rampant Sale of Fake Documents*, CHI. SUN-TIMES, Aug. 26, 1996, at 18 (discussing the market for and traffic in false identification documents); *INS Raid Snares $80 Million in Bogus Immigration Documents*, NOTARY BULL., Feb. 1999, at 13 ("More than two million documents were discovered by INS agents, including driver's licenses from California and eight other states, Social Security cards, Mexican birth certificates and green cards.").

80. *See, e.g.*, First Bank of Childersburg v. Florey, 676 So.2d 324 (Ala. Civ. App. 1996) (noting that the family member who forged the signature of her father-in-law had commented that she could "sign [his name] as well as he can"); *see also* the sample of cases in which forgeries were successfully perpetrated upon notaries: McDonald v. Plumb, 12 Cal. App. 3d 374, 90 Cal. Rptr. 822 (1970); Independence Leasing Corp. v. Aquino, 133 Misc. 2d 564, 506 N.Y.S.2d 1003 (Sup. Ct. 1986); Iselin-Jefferson Financial v. United California Bank, 549 P.2d 142 (Cal. 1976). Con-artists have been so successful recently at the process called identity theft that Congress has enacted a new felony statute to deal with the problem. *Identity Theft Now a Felony Under New Federal Law*, NAT'L NOTARY, Jan. 1999, at 25. Furthermore, the risks to the employers of notaries resulting from their vicarious liability for the negligence of notary-employees is part of the reason for the move in some states to permit employers and notaries to restrict or prohibit the performance of notarial services during the hours of employment and/or to limit such services only to customers of

Most importantly, traditional notaries do not play any role in validating the substance of documents. Signatures are notarized; documents are not.[81] Hence, a real document signer (not an impostor) might present a forged or altered instrument for signing and notarization of the signature.[82] When this happens, the notary has no responsibility to detect the substantive defect of the instrument (with the possible exceptions of cases involving blind and illiterate signers).[83] Moreover, after the signature has been notarized, the document may very well be altered before presentment to another party.[84] A traditional notary certainly cannot prevent such subsequent misconduct.

To cope with the enormous volume of commercial and governmental instruments required to be notarized,[85] the number of notaries in this

---

the employer. *See* Closen, *supra* note 61, at 676-681, 685-688 (discussing both vicarious liability and the limitation of notarial services [the "notary private" concept]); *Legislative Review,* NOTARY BULL., Feb. 1999, at 6, 7 (pointing out that New Jersey has adopted a new law allowing notaries employed by financial institutions "to refuse to administer an oath to any person while on the employer's premises or during the . . . hours of employment").

81. *See* Klint L. Bruno & Michael L. Closen, *Notaries Public and Document Signer Comprehension: A Dangerous Mirage in the Desert of Notarial Law and Practice*, 44 S.D. L. REV. (1999) [forthcoming]; Closen & Dixon, *supra* note 45, at 889 ("By witnessing a signature, the notary is not attesting to the validity or legal effect of the document on which the signature appears."); Klint L. Bruno, Comment, *To Notarize, Or Not To Notarize . . . Is Not a Question of Judging Competence or Willingness of Document Signers*, 31 J. MARSHALL L. REV. 1013 (1998).

82. *See, e.g.*, Facey v. Dept. of State, 132 A.D.2d 698, 518 N.Y.S.2d 177 (1987) (stating that the signer did not personally appear before notary and that the document contained false information); McWilliams v. Clem, 743 P.2d 577 (Mont. 1987) (stating that the husband, who signed a deed, persuaded the notary to also notarize the purported signature of the wife to the same deed although the wife was not present, and that the wife's signature was a forgery); Butler v. Comic, 918 S.W.2d 697 (Ark. 1996) (stating that two of ten brothers and sisters presented a quitclaim deed purportedly signed by all ten to a notary for notarization even though eight were not present, and that some of the signatures were forgeries); Ameriseal of North East Florida Inc. v. Leiffer, 673 So.2d 68 (Fla. App. Ct. 1996) (stating that a notary notarized the actual signatures of two document signers although they were not present and that the document contained false information). Indeed, it could even be that the notary might tamper with a document after it had been notarized, as was so in the case of State v. Maryland Casualty Company, 344 S.W.2d 55 (Mo. 1961).

83. *See* 5 I.L.C.S. 312/6-104(e) ("A notary public shall not take the acknowledgment of any person who is blind until the notary has read the instrument to such person."). *See also* 66 C.J.S. NOTARIES § 6(c) ("With respect to contracts, an instrument executed by the parties before a notary in the presence . . . of three witnesses if a party be blind, is an 'authentic act,' and is full proof of the agreement contained in it.").

84. *See, e.g.*, D.T. Parker, Notary Lawsuits [letter], NOTARY BULL., Feb. 1999, at 4 ("One of my employees legitimately notarized a document for a customer, who then utilized a photocopier to transfer her signature and seal impression to another document and commit real estate fraud.").

85. Many documents are notarized needlessly because no notarization requirement exists. NOTARY LAW & PRACTICE, *supra* note 63, at 135. *See, e.g.*, Estate of Peterson, 579 N.W.2d 488 (Minn. App. Ct. 1998) (holding that a purported "contract" which had been

country has grown quite steadily.[86] There are now more than 4.2 million notaries public,[87] which exceeds the population of about 30 states.[88] What this means is that there are more notaries than there are lawyers, police officers, doctors and dentists, primary and secondary school teachers, and active duty military personnel.[89]

Remarkably, handwritten signatures affixed to documents while in the physical presence of notaries and while in the home states of the notaries have worked fairly effectively thus far.[90] But, there is room for fraud. Although the use of handwritten signatures by signers who have been required to appear in the physical presence of notaries has served government and commerce, the world to be dominated by e-mail and the Internet will be inhospitable to these old-fashioned methods. It will not be possible or efficient to obtain presently hand-scrawled signatures; it will not be possible or efficient to insist upon face-to-face meetings; and it

---

notarized was not a contract at all). Moreover, criminal and civil penalties already exist for forgery or document falsification. Closen, *supra* note 59, at A23.

86. Closen, *supra* note 59, at A23.

87. *Id.*

88. *Id.*

89. *Id.*

90. Since the purpose of the notary public has been to prevent fraud in the execution of written paper documents by exercising reasonable care to properly identify document signers, it has been accepted that physical appearance by the signer in the presence of the notary was necessary. *See generally* Charles N. Faerber, *Being There: The Importance of Physical Presence to the Notary*, 31 J. MARSHALL L. REV. 749 (1998). Moreover, since physical appearance was required and since each state and territory has so many notaries available, this system has been efficient and effective. Limiting the authority of notaries to the physical boundaries of their home states or territories has seemed appropriate, too. But even this latter practice has been eroded in recent years by states that allow non-residents to hold notary commissions if they work there (although the individuals live in neighboring states) and that grant reciprocity to notaries (provided the notaries' home states do likewise). *See* Douglass M. Fischer, *Where Can I Notarize?*, NAT'L NOTARY, July 1997, at 10 (containing an extensive discussion indicating each state's notarial jurisdiction practices). Furthermore, a key advantage of electronic documents endorsed by digital signatures should include the absence of a need for the signers to meet face-to-face themselves or with a third party such as a certification authority. *See* Closen & Richards, *supra* note 4, at 729. With the new technologies of video conferencing and facsimile and computer transmissions of documents, the necessity of the old-fashioned requirement of physical presence before a notary has been questioned. *See* NOTARY LAW AND PRACTICE, *supra* note 63, at 24-25 (setting out two hypothetical problems about signatures executed during a video conference and immediately faxed to a notary). *See also* Glen-Peter Ahlers, *The Impact of Technology on the Notary Process*, 31 J. MARSHALL L. REV. 911, 922-924 (1988) (discussing interactive video). Furthermore, a key advantage of electronic documents endorsed by digital signatures should include the absence of a need for the signers to meet face-to-face themselves or with a third party such as a certification authority. *See* Closen & Richards, *supra* note 4, at 729. Of course, the jurisdictional consequences of electronic commerce will prove to be complex and controversial. *See* Hope Viner Samborn, *Small World, Big Questions*, A.B.A. J., Feb. 1999, at 78 ("In the case of electronic commerce, a number of jurisdictions may have the right to assert their substantive laws upon electronic transaction disputes.").

will not be efficient to restrict certification authorities operating on-line in cyberspace to traditional geographical statewide boundaries.

III. OVERVIEW OF DIGITAL SIGNATURE TECHNOLOGY

The Internet is also known as the "information superhighway." As the nickname implies, it is an extraordinary tool for accessing information, but a poor one for securing it. As an "open network," electronic documents and other data may pass through countless interconnected computers on their Internet voyage,[91] and the possibility that their contents may be tampered with is fairly high.[92] This problem intensifies the need for a dependable authentication system. Digital signatures verified by certification authorities fill a void that handwritten signatures verified by traditional notaries cannot on the Internet, and are perhaps more useful at accomplishing authentication tasks than their handwritten counterparts.[93]

"A secure digital signature is believed to be the key to allowing technology to further revolutionize electronic commerce."[94] It accomplishes this goal in several ways. First, like a handwritten signature, a digital signature should identify a document's signer, and it should be difficult to reproduce without permission.[95] Second, a digital signature verified by a certification authority ensures the integrity of the document itself, making it impossible or impracticable to alter it or its contents without detection.[96] While a handwritten signature at the end of a contract truly authenticates only the last page, a digital signature verified by a certifi-

91. *See* A.C.L.U. v. Reno, 929 F. Supp. 824, 830-49 (E.D.Pa. 1996) (discussing the characteristics of the Internet).

92. 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, 310-11 (1997).

93. Anthony Martin Singer, Note, *Electronic Commerce: Digital Signatures and the Role of the Kansas Digital Signature Act*, 37 WASHBURN L.J. 725 (1998). Because of the binding between a sender and the signed message, a digital signature provides a higher degree of security and authenticity than a handwritten signature. Randy V. Sabett, *International Harmonization in Electronic Commerce and Electronic Data Interchange: A Proposed First Step Toward Signing On the Digital Dotted Line*, 46 AM. U. L. REV. 511, 521 (1996).

94. Elizabeth Wasserman, *Signing On With Digital Signatures New Laws May Allow Computer Validation*, PHOENIX GAZ., Aug. 29, 1995, at A1, *available in* 1995 WL 2824237.

95. Information Security Committee, Electronic Commerce Division, *Digital Signature Guidelines*, 1996 A.B.A. SEC. SCI. & TECH. 13 [hereinafter *Digital Signature Guidelines*].

96. *Id.* at 6-7. Because a digital signature uses the actual text of the message when formulating the encryption algorithm, the slightest alteration will prevent the message from decrypting properly. A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 54 (1996). "Two things happen to make a digital signature valid: A digital snapshot of the document is taken; and a signature, based on the user's certificate, is created." Klau, *supra* note 6, at 14.

cation authority authenticates the entire document down to the last punctuation mark.[97] Third, a digital signature verified by a certification authority eliminates the possibility of repudiation by the sender.[98] Finally, electronic documents can be encoded with a digital time stamp, allowing the transmission time to be ascertained.[99] Such non-repudiation features not only assure the recipient that the sender cannot falsely deny that the document was sent, but also prevent either party from unilaterally altering the terms of an agreement.[100] These technological devices should make electronic document certification a safe and reliable means for ensuring security during an electronic transaction.

A digital signature is not a computerized image of a handwritten signature.[101] Rather, a "digital signature" is a phrase of art describing a systematic scrambling of characters to guarantee security and authenticity.[102] More specifically, digital signatures are created and verified through the use of cryptography, ensuring the authenticity of an electronic document's content and the sender's identity[103] The cryptographic process used to create digital signatures is currently known as "public key cryptography."[104] This process involves the use of an algorithm using two distinctly separate but mathematically related "keys," or a "keypair."[105] A private key, held only by the sender, is used to generate the digital signature and convert the document into an unintel-

97. Sabett, *supra* note 93, at 521. To analogize, imagine that the parties to a contract were to sign their names to each and every character on a contract. *Id.* Cases where signed documents were altered do arise. *See, e.g.*, Zion's First Nat'l Bank v. Rocky Mountain Irrigation, Inc., 795 P.2d 658 (Utah 1990); Citizens Nat'l Bank of Downers Grove v. Mormon, 398 N.E.2d 49 (Ill. App. Ct. 1979); Newell v. Edwards, 173 S.E.2d 504 (N.C. Ct. App. 1970).

98. Suppose, for example, that a party sends an offer to enter into a contract, and the offeree accepts. Later, the offeror tries to deny that the offer was ever made. The offeree can prove the offer's existence by using the offeror's public key to decrypt the document. This would eliminate the possibility of repudiation, since only the offeror's private key could have created the original encrypted message. *See* Sabett, *supra* note 93, at 522.

99. A digital time stamp provides an extra measure of security should a private key become compromised. For further discussion of digital time stamping. *See* DAVE BAYER, ET AL., IMPROVING THE EFFICIENCY AND RELIABILITY OF DIGITAL TIME-STAMPING, IN SEQUENCES II: METHODS IN COMMUNICATION, SECURITY, AND COMPUTER SCIENCE (Renato Capocelli, et al. eds., 1993).

100. *Digital Signature Guidelines*, *supra* note 95, at 7.

101. Greenwood & Campbell, *supra* note 92, at 310.

102. MICROSOFT PRESS COMPUTER DICTIONARY 145 (3d ed. 1997).

103. *Digital Signature Guidelines, supra* note 95, at 8. Cryptography is a mathematical process that scrambles documents into an unintelligible form (known as encryption) and then converts them back again (known as decryption). *Id.*

104. *Id.*

105. *Id.* Hardware and Software using this two key system are collectively referred to as an "asymmetric cryptosystem." *Id. See also* Hill, *supra* note 4, at 10. Asymmetric cryptosystems function at a slower rate than symmetric cryptosystems (which use the same

ligible form.[106] A corresponding public key is used to transform the document back to its original form.[107] Reliability and authenticity is thus ensured, because the keys operate together in such a way that the digital signature generated by the private key cannot be practicably decrypted by any key other than the public key belonging to the sender (much like two interlocking secret decoder rings from a cereal box, provided they are unique).[108] The sender's public key is made accessible to all who need it by posting it on a Web site or some other type of directory or repository provided by the Certification Authority.[109]

Suppose diamond buyer Jean wanted to send a digitally signed message to diamond seller Carroll. How would Jean go about doing so? First, Jean would draft the document[110] and then send it through a mathematical algorithm called a hash function,[111] which would produce a number known as a "hash value" or "hash result."[112] Jean would next

---

key to encrypt and decrypt), but are more secure. *See* GONCALVES, *supra* note 35, at 608, 620.

106. *Digital Signature Guidelines*, *supra* note 95, at 8. *See also* Klau, *supra* note 6, at 14 ("[T]he individual keeps the private key in a safe place on his or her disk drive and uses it to sign documents.").

107. *Digital Signature Guidelines*, *supra* note 95, at 8.

108. R.J. Robertson, Jr., *Electronic Commerce On the Internet and the Statute of Frauds*, 49 S.C. L. REV. 787 (1998).

109. *Digital Signature Guidelines*, *supra* note 95, at 8. *See also* Hill, *supra* note 4, at 10 ("Although the public key may be restricted to only one or a few users, it is usually made publicly available through an online repository that is operated by an independent party . . . " known as a certification authority;) Klau, *supra* note 6, at 14 ("The public key is distributed to all correspondents . . . .").

110. Digital signatures appear as gibberish, a mere stream of characters. *See* Sabett, *supra* note 93, at 521. A digitally signed message might look like this:

— BEGIN SIGNED MESSAGE —
Name: Chicago Widget Corp.
Order No. 2523
Date: June 2, 1999
This document is an order for 500 blue widgets at the price of $100/each.
— END SIGNED MESSAGE —
Public ID# 7Y4737Y34874
Public key available at:
http://www.certification_authority.com/chicagowidget/publickey.html
— BEGIN SIGNATURE —
I86T7887tj76UJSLkj78342gd56ET445e098Ujhf65R987yur5UpFTf4ERD897gW
35YfdlOAfavg4tggg54fglIJG23o9kj120goND1998
— END SIGNATURE —

Id. at 520-21.

111. Hash functions are used to both generate and verify digital signatures. *See Digital Signature Guidelines*, *supra* note 95, at 9.

112. *Id.* This hash value or hash result is unique to the digitally signed message. *Id.* If the message were tampered with in any way, a different hash result would be produced, signifying alteration. *Id.* A hash value or hash result is a mathematical algorithm used to create a unique "fingerprint" known as a "hash value" or "hash result." The hash value, or hash result, has also been called a "message digest." *See* Greenwood & Campbell, *supra*

encrypt the hash result with a private key, thus, forming the electronic document and digital signature.[113] The document could then be electronically mailed directly to Carroll. After receiving the document, Carroll can verify Jean's identity by decrypting the digitally signed document using Jean's public key.[114] If successful, Carroll most likely can be confident that Jean is the actual sender of the document.[115] To confirm that the document has not been tampered with, Carroll can use the same hash function that Jean used earlier.[116] If the two-hash results match, the document would appear not to have been altered,[117] and the parties can be somewhat assured that the integrity of the document has not been compromised. However, the question still remains as to how parties might more reliably identify a key pair to the entity with which they are communicating.[118]

At this stage the certification authority's role becomes paramount.[119] For heightened security and reliability, the communication from Jean to Carroll could be sent through the trusted intermediary of a certification authority. Certification authorities have several duties, including key pair management, as well as overseeing issuance, distribution, suspension and revocation of digital certificates.[120] The certification authority acts as a trustworthy third party by assigning key pairs and digital certificates that verify the sender's identity.[121] The cer-

---

note 92, at 314 (describing a substantially similar sequence). The possibility of ascertaining a private key by accessing the hash result has been termed "computationally infeasible." *Digital Signature Guidelines, supra* note 95, Tutorial, at 9. This is a relative concept, however, based on several factors including the data's value, the length of time and money expended, and future technological advances. *Id.* at 8 n.23.

113. Greenwood & Campbell, *supra* note 92, at 314. At this point Sara's identity as the sender is "stamped" onto the document and established for purposes of authentication. *Id.* at 314 n.15.

114. *Id.* at 314.

115. *Id.*

116. *Id.*

117. *Id.*

118. Greenwood & Campbell, *supra* note 92, at 314. Conceivably, a criminal could generate a key pair and fraudulently claim that it belongs to Sara Sender. *Id.*

119. One such service provider is a company called VeriSign, Inc. VeriSign provides digital certificates of varying types, from the "Class 1" certificate for casual web and e-mail use to the ultra-secure "Class 4," issued only after a thorough investigation. The site is located at <http://verisign.com>.

120. INFORMATION SECURITY COMMITTEE, SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOCIATION, TUTORIAL, 38 JURIMETRICS J. 243, 254 (1998).

121. Froomkin, *supra* note 96, at 55. "A certificate is a digitally signed statement by a certification authority that provides independent confirmation of an attribute claimed by a person proffering a digital signature." *Id.* A certificate should include: (1) the identification and digital signature of the certification authority; (2) identifies or names the subscriber; (3) identifies the certificates valid operational period; and (4) provides the subscriber's public key. *See Digital Signature Guidelines, supra* note 95, at 29.

tificate identifies the public key as "the subject of the certificate" and verifies that the sender identified by the certificate controls the matching private key.[122] A certificate may typically contain the identity of the issuing certification authority, identification of the subscriber, the subscriber's public key, and the digital signature of the certification authority.[123] It might also contain additional information, such as a certificate's expiration date, a statement of the certification authority's financial responsibility (or at least a reference to see the authority's repository for a detailed statement of financial responsibility), or the context in which the public key may be used.[124] The certificate is then made available in a repository or on the certification authority's Web site.[125] The digitally signed document's recipient may then access the sender's certificate, access a copy of the sender's public key, and decrypt the document.[126] Thus, the receiver can rest assured that the sender is indeed who he or she purports to be, and that the document has not been altered.[127]

The security of a private key might be compromised, for example, where an unauthorized person obtained the private code.[128] This failure of security could result from lack of diligence by the private key holder and/or from fraudulent practice by the unauthorized user.[129] The America Online e-mail disruption, cited earlier,[130] illustrates that inattention to security can be a most serious problem in electronic commerce. The American Bar Association developed an extensive set of Digital Signature Guidelines, which address this problem in several ways.[131] First, the private key-holding subscriber is held to a duty of care in its safekeeping.[132] Second, the private key-holder should be enabled to "disas-

122. Robertson, *supra* note 108, at 787.

123. Greenwood & Campbell, *supra* note 92, at 315.

124. Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1202 (1998).

125. *Id.* A repository is an online database of certificates and is used to verify digital signatures. *See Digital Signature Guidelines*, *supra* note 95, at 19.

126. Robertson, *supra* note 108, at 787.

127. *Id.*

128. *See id.* at 732-734 (discussing the "alarming increase in computer-generated fraud" and the security problems associated with "inadequate identification procedures" for computer users).

129. *See id.* at 737 ("The only way that a digital signature's integrity should be subject to compromise is if the private key holder is negligent in safeguarding the key, or intentionally gives others access to the signature software and provides them with the passphrase.").

130. *See supra* notes 18-23 and accompanying text.

131. *Digital Signature Guidelines*, *supra* note 95, Tutorial, at 8 n.20.

132. *Id.* The sender has several methods at his disposal to safeguard the private key. A particularly safe method is the use of a "cryptographic token" (a "smart card," for example). *Id.* This device activates the signature program using an internal microchip, allowing the

sociate himself from the key by temporarily suspending or permanently revoking his certificate and publishing these actions in a 'certificate revocation list,' or CRL."[133] Other possibilities to ensure security are dating certificates when they are issued, and limiting their period of validity.[134] The certificate should give explicit reference to the CRL, insisting that it be checked regularly.[135] Individual receivers might decide to accept certificates issued in the last few days, or will have to determine which certification authorities are the most reputable, trustworthy, and financially responsible.[136] Also, a certification authority "must utilize trustworthy systems in performing its services."[137] To ensure that all statutory guidelines are followed closely, both the Utah and Washington statutes require that a certified public accountant with expertise in computer security audit each certification authority's records at least once per year.[138] Finally, the entities (and in particular the people) who will perform electronic document verifications must be free from corrupt influences.

How do we protect ourselves against fraudulent certification authorities? Or suppose a certification authority's system is compromised? One certification authority can verify the authenticity of another certification authority, or a certificate issued by another certification authority.[139] However, in this hierarchy situation, a certification authority will ultimately exist that is not verified by another.[140] "Cybernotaries that certify other Cybernotaries are said to participate in a certificate chain, with a root certificate at the bottom of the tree."[141] Clearly, there must be a root certification authority that will instill the highest degree of confidence among certification authorities, subscribers and relying parties who are higher in the tree.[142] Utah's digital signature statute autho-

---

document to be signed without the private key ever being divulged outside the token, nor does it enter the sender's computer memory. *Id.* The sender is required to physically produce the token, and security measures such as a fingerprint scan can verify the physical presence of the token's proper holder. *Id.*

133. *Digital Signature Guidelines*, *supra* note 95, Tutorial, at 8 n.20.

134. Froomkin, *supra* note 96, at 61.

135. *Id.*

136. *Id.*

137. *Digital Signature Guidelines*, *supra* note 95, § 3.1; WASH. REV. CODE ANN. § 19.34.100 (Supp. 1998).

138. *See* WASH. REV. CODE ANN. § 19.34.110 (Supp. 1998); *see* UTAH CODE ANN. § 46-3-202 (Supp. 1996).

139. Winn, *supra* note 124, at 1202. *See also* Hill, *supra* note 4, at 11 ("How does a recipient know that the certification authority isn't an impostor? The recipient can verify the authority's digital signature using a public key on another public certificate . . . .").

140. Hill, *supra* note 4, at 11.

141. Froomkin, *supra* note 96, at 56, (citing Warwick Ford, *Advances in Public-Key Certificate Standards*, SIG SECURITY, AUDIT & CONTROL REV., July 1995, at 9, 10).

142. Winn, *supra* note 124, at 1202.

rizes the state to act as the root authority by regulating certification authority licensing.[143] Other states may adopt this approach as well, hopefully rewarding only a few certification authorities with licenses after conforming to strict guidelines.[144]

IV. THE NOTARY PUBLIC MODEL

There are several parallels between the positions of the traditional notary public and the certification authority. Indeed, those similarities have appeared so strong that, as noted previously, the two positions even share a common title within the shorthand reference "cybernotary."[145] However, the central question of this paper is whether the notary should really serve as the model for the certification authority. The authors have concluded that the differences between the two positions far outweigh their commonalities, and that sound business and legal policy warrant distancing the position of certification authority from the wholly unsatisfactory notary model.

Both notaries public and certification authorities are creatures of statute. That is, both positions are created and regulated by statute.[146] While every state sets forth fairly detailed statutory guidelines for notaries,[147] only a handful of jurisdictions have passed extensive digital sig-

143. *See* UTAH CODE ANN. §§ 46-3-201 to 46-3-504 (1997).

144. Froomkin, *supra* note 96, at 56, (citing UTAH CODE ANN. §§ 46-3-104 to 46-3-201).

145. Florida has even adopted the country's first statute creating an amended notary commission for notaries who wish to become qualified to perform "electronic notarizations" by signing with their "digital signatures" registered with a Florida certification authority. *See* FLA. STAT., § 117.20.

146. Closen, *supra* note 61, at 651 (noting the statutory origin of the office of notary public); Closen & Richards, *supra* note 4, at 739 (noting that digital signatures and certification authorities are authorized by statutes).

147. *See* ALA. CODE §§ 36-20-1 to 32 (1991); ALASKA STAT. §§ 44.50.010 to 190 (Michie 1996); ARIZ. REV. STAT. ANN. §§ 41-311 to 317 (West 1992 & Supp. 1995); ARK. CODE ANN. §§ 21-14-101 to 05 (Michie 1996 & Supp. 1996); CAL. GOV'T CODE §§ 8200-8230 (West 1992 & Supp. 1997); COLO. REV. STAT. ANN. §§ 12-55-101 to 123 and 12-55-201 to 211 (West 1996); CONN. GEN. STAT. ANN. §§ 3-91 to 95a and 7-33a (West 1988 & Supp. 1996); DEL. CODE ANN. tit. 29, §§ 4301 to 4401 (1991 & Supp. 1996); D.C. CODE ANN. §§ 1-801 to 817 (1992); FLA. STAT. ANN. §§ 117.01 to 108 (West 1996 & Supp. 1997); GA. CODE ANN. §§ 45-17-1 to 34 (Harrison 1990 & Supp. 1996); HAW. REV. STAT. §§ 456-6 to 18 (Michie 1995 & Supp. 1995); IDAHO CODE §§ 51-101 to 123 (1994); 5 ILL. COMP. STAT. 312/1-101 to 8-104 (West 1993 & Supp. 1996); IND. CODE ANN. §§ 33-16-1-1 to 16-8-5 (Michie 1992 & Supp. 1996); IOWA CODE ANN. § 586.1 (West 1992); Kan. Stat. Ann. §§ 53-101 to 401 (1983); KY. REV. STAT. ANN. §§ 423.010 to 990 (Michie 1992 & Supp. 1996.); LA. REV. STAT. ANN. §§ 35:1 to 555 (West 1985 & Supp. 1997); ME. REV. STAT. ANN. tit. 4, §§ 951 to 958 (West 1989 & Supp. 1996); MD. ANN. CODE art. 68, §§ 1 to 13 (1995 & Supp. 1996); MASS. GEN. LAWS ANN. ch. 222, §§ 1 to 11 (West 1993 & Supp. 1996); MICH. COMP. LAWS ANN. §§ 5.1041 to 5.1072 (West 1993 & Supp. 1996); MINN. STAT. ANN. §§ 359-01 to 12 (West 1991 & Supp. 1997); MISS. CODE ANN. §§ 25-33-1 to 23 (1991 & Supp. 1996); MO. ANN. STAT. §§ 486-100 to 595 (West 1995 & Supp. 1997); MONT. CODE ANN. §§ 1-5-201 to 611 (1995); NEB. REV. STAT.

nature legislation at this time.[148] However, commentators predict that every state will pass digital signature legislation over the next decade.[149] To date, the same governmental agencies that oversee notaries have tended to be designated as the agencies to supervise certification authorities.[150] Most often, those agencies are the Secretary of State's offices.[151] The statutes establishing both positions usually treat many of the same topics, including such matters as application procedures,[152] qualifications,[153] financial responsibility,[154] fees or fee schedules,[155] du-

---

§§ 64-101 to 215 (1990); NEV. REV. STAT. ANN. §§ 240.001 to 330 (Michie 1996); N.H. REV. STAT. ANN. §§ 455:1 to 15 (1992 & Supp. 1995); N.J. STAT. ANN. §§ 52:7-10 to 21 (West 1986 & Supp. 1996); N.M. STAT. ANN. §§ 14- 12-1 to 20 (Michie 1995); N.Y. EXEC. LAW §§ 6-130 to 38 (McKinney 1993 & Supp. 1997); N.C. GEN. STAT. §§ 10A-1 to 16 (1991); N.D. CENT. CODE §§ 44-06-01 to 14 (1993 & Supp. 1995); OHIO REV. CODE ANN. §§ 147.01 to 14 (Banks-Baldwin 1994 & Supp. 1996); OKLA. STAT. ANN. tit. 49, §§ 1 to 121 (West 1988 & Supp. 1997); OR. REV. STAT. §§ 194.005 to 990 (1991); 57 PA. CONS. STAT. ANN. §§ 31 to 169 (West 1996); R.I. GEN. LAWS §§ 42-30-1 to 15 (1993 & Supp. 1996); S.C. CODE ANN. §§ 26-1-10 to 120 (Law Co-op. 1991 & Supp. 1996); S.D. CODIFIED LAWS ANN. §§ 18-1-1 to 14 (Michie 1995); TENN. CODE ANN. §§ 8-16-101 to 309 (1994); TEX. GOV'T CODE ANN. §§ 406.001 to 024 (West 1990); UTAH CODE ANN. § 46-1-1 to 19 (1993 & Supp. 1996); VT. STAT. ANN. tit. 24, §§ 441 to 446 (1992); VA. CODE ANN. §§ 47.1-1 to 33 (Michie 1996 & Supp. 1996); WASH. REV. CODE ANN. §§ 42.44.010 to 903 (West 1991 & Supp. 1997); W.VA. CODE §§ 29-4-1 to 16 (1992 & Supp. 1996); WIS. STAT. ANN. § 137.01 (West 1989 & Supp. 1996); WYO. STAT. §§ 32-1-101 to 113 (Michie 1996).

148. *See, e.g.*, Arizona (ARIZ. REV. STAT. ANN. §§ 41-121 (West Supp. 1997)); California (CAL. GOV'T CODE § 16.5 (West Supp. 1998)); Connecticut (CONN. GEN. STAT . §§ 19a-25a (1997)); Florida (FLA. STAT. ANN. §§ 282.70 to 75 (West Supp. 1998)); Iowa (IOWA CODE § 48A.13 (Supp. 1998)); Kansas (KAN. STAT. ANN. § 60-2616 (Supp. 1997)), Louisiana (LA. REV. STAT . ANN. § 40:2144 (West Supp. 1998)); Minnesota (MINN. STAT. § 221.173 (Supp. 1998)); Mississippi (MISS. CODE ANN. §§ 25- 63-1 to 11 (Supp. 1997)); New Mexico (N.M. STAT. ANN §§ 14-15-1 to 6 (Michie Supp. 1997)); Utah (UTAH CODE ANN. §§ 46-3-101 to 504 (Supp. 1997)); Virginia (VA. CODE ANN. §§ 59.1-467 to 469 (Michie Supp. 1997)); Washington (WASH. REV. CODE ANN. §§ 19.34.010 to 903 (West Supp. 1998)); and Wyoming (WYO. STAT. ANN. § 9-1-306 (Michie 1997)).

149. Charles N. Faerber, *Electronic Notarization: Florida, Utah Lead the Way*, THE NAT'L NOTARY, July 1998, at 21.

150. *See supra* note 40 (discussing state agencies that monitor both notaries and certification authorities).

151. Closen & Richards, *supra* note 4, at 719 (*citing* ARIZ. REV. STAT. ANN. § 41-311 (1992); ARK. CODE ANN. § 21-14-101 (Michie 1996); CAL. GOV'T CODE § 8200 (West 1992); COLO. REV. STAT. § 12-55-104 (West 1996); CONN. GEN. STAT. ANN. § 3-91 (West 1988 & Supp. 1996); IOWA CODE ANN. § 77A.3 (West 1992); KAN. STAT. ANN. § 53- 102 (Michie 1992); KY. REV. STAT. ANN. § 423.010 (1992); N.J. STAT. ANN. § 52:7-11 (West 1986 & Supp. 1996); N.Y. EXEC. LAW § 130 (McKinney 1993 & Supp. 1996).

152. *See* 152 ILL. COMP. STAT. 312/2-101 to 106.

153. *Id.* at 312/2-102.

154. *Id.* at 312/2-105.

155. *See, e.g.*, UTAH CODE ANN. § 46-1-12 (Supp. 1997) (setting notary fees at $5); *see also* WASH. REV. CODE ANN. § 19.34.040 (West Supp. 1998) (allowing secretary of state to establish reasonable fees for electronic document certification services).

ties,[156] misconduct,[157] and discipline.[158]

Further, as already noted, both notaries public and certification authorities possess the professional and legal duty to accurately identify document signers (without guaranteeing the proper identity of those signers).[159] Like the traditional notary, the certification authority will play a critical role in business transactions where a third party is needed to authenticate signatures.[160] In a fast changing global electronic marketplace, there are few constants. Yet, among them are the pervasive problems of dishonesty and fraud,[161] and the likelihood of dealing with anonymous people in far away parts of the world.[162] More than ever before, it is essential that parties have confidence in the identities of their counterparts to transactions.[163] It is only at this point that the parties may "proceed under an umbrella of trust."[164] Hence, the notary and certification authority will share the same identity verification purpose. Those are the common features of the two positions.

---

156. *See* ILL. COMP. STAT. 312/3-101 to 4-101.

157. *See, e.g.*, MODEL NOTARY ACT, § 6-203 (1984) (allowing for criminal prosecution of notarial misconduct; *see also* WASH. REV. CODE ANN. § 42.44.160 (West 1991) (making notarial conduct a gross misdemeanor); WASH. REV. CODE ANN. § 19.34.502 (Supp. 1998) (stating that certification authority may be subject to both injunctive relief and criminal prosecution for misconduct).

158. *See, e.g.*, MODEL NOTARY ACT § 6-201 (1984) (giving state power to revoke a notarial commission); *and* WASH. REV. CODE ANN. § 42.44.170 (West 1991) (allowing state to revoke notary's appointment); *see also* WASH. REV. CODE ANN. § 19.34.400 (allowing secretary of state to discontinue recognition of certificate repository).

159. Notaries have never been legally expected to serve as guarantors of the identities of document signers, but merely to act with reasonable care in the process of identifying signers. *See* NOTARY LAW INSTITUTE, *supra* note 74, at 4 ("[T]he notary does not 'guarantee' the signature [of the document signer] is not a forgery.") *Id.* "A notary is required to exercise reasonable care in verifying a signer's identity and to ensure the signature being notarized belongs to the person appearing before her. If the notary exercises reasonable care in making those determinations, she cannot be held liable." *Id.* at 5.

160. *See generally* Froomkin, *supra* note 96 (discussing the importance of a certification authority).

161. *See* Wendy Lee, *Intensifying Efforts Against Internet Piracy*, NEW STRAITS TIMES, Apr. 23, 1998, at 4, *available in* 1998 WL 3977488. The Federal Trade Commission's Bureau of Consumer Protection was not laughing recently when a con-artist began selling franchises for the fictional "U.S. Consumer Protections Agency" over the Internet at $6000. Richard Wolffe, *FTC Not Amused By Internet Ad Offering To Franchise Its Agency*, THE PLAIN DEALER, July 4, 1998, at 8A, *available in* 1998 WL 4143099. In 1997, the FTC uncovered a fraudulent $30 million Internet business deal. *Id.*

162. A New Yorker cartoon quips "On the Internet, they can't tell you're a dog." Charles R. Merrill, *An Attorney's Roadmap to the Digital Signature Guidelines*, 452 PLI/P, at 379, 382 (1996).

163. William A. Reinsch, *Should Uncle Sam Control U.S. Encryption Technology Exports?*, INSIGHT, Sept. 8, 1997, at 24, *available in* 1997 WL 11444408.

164. Chuck Appleby, *Encryption Making Security A Reality*, 508 INFO. WK., Jan. 2, 1995, at 38, *available in* 1995 WL 7138713.

By contrast, the differences between the two posts are far more substantial both in quantity and quality. Foremost among the differences is that a notary public is a commissioned public official,[165] a public servant with a long tradition of fiduciary responsibility to the citizenry[166] and with a duty to be reasonably available to service all members of the public without discrimination[167]—including without limiting notarial service only to customers or clients of the notary or the notary's employer.[168] Thus, the title is notary public, not notary private.[169] While the state issues licenses to all sorts of others, such as vehicle drivers,[170] private detectives,[171] attorneys,[172] barbers and beauticians,[173] pharmacists,[174] real estate brokers,[175] morticians,[176] gun owners,[177] and so on,[178] these others do not become public officers the way that notaries do.[179] At most, certification authorities should be licensed by the state just as so many others are licensed to provide a basis for state oversight and public protection and to assess the subject matter of the license for revenue reasons. Beyond those basic purposes, market forces can and should drive the private sector functioning of certification authorities. Most assuredly, certification authorities do not need to be public officials.

There are a couple of other functions of certification authorities not possessed by notaries. The traditional notary essentially affixes his/her signature and seal, and the transaction is complete. Once the notarization on a paper document takes place, the process is completed.[180] Any

165. Closen, *supra* note 59, at A23 ("Notaries are not merely licensed, they are almost always commissioned by elected officials such as the state governor or the secretary of state.").

166. Closen, *supra* note 61, at 657 (quoting Humphrey's 1948 book to the effect that "[o]fficially a notary public is the agent of the public only . . . ."). The notary has been a public servant or public official since ancient times. *See* Closen & Dixon, *supra* note 45, at 874-875.

167. Closen, *supra* note 61, at 685-689.

168. *Id.* at 687-688.

169. *Id.* at 685.

170. 65 ILL. COMP. STAT. 5/6-101 et seq.

171. *Id.* at 5/11-42-1.

172. 70 ILL. COMP. STAT. 205-1.

173. 65 ILL. COMP. STAT. 5/11-42-1.

174. 225 I.L.C.S. 85/6 et seq.

175. *Id.* at 455/2 et seq.

176. *Id.* at 41/5-5 et seq.

177. 430 ILL. COMP. STAT. 65/2 et seq.

178. *See* 65 ILL. COMP. STAT. 5/11-42-6; *see also* 65 ILL. COMP. STAT. 5/11-42-2.

179. *See generally* Closen, *supra* note 61 (discussing the public notary).

180. Douglas M. Fischer, *Cancel a Notarization?*, THE NAT'L NOTARY, Sept. 1995, at 12. Moreover, the relationship between the notary and document signer for whom a notarization is performed is usually quite short. *See* Closen, *supra* note 61, at 661, 669. Its brevity is one of the reasons why some reject the notion that a signer-notary relationship can be a principal-agent or fiduciary relationship. *Id.* at 669.

oversights or errors cannot be corrected, nor can the notarization be "taken back" if an error is discovered.[181] In contrast, certification authorities not only may, but must subsequently suspend or revoke a certificate in such comparable situations.[182] Unlike a notary, the certification authority must continue to watch for fraud even after the document is authenticated. A certification authority must suspend or revoke a certificate if the certification authority confirms that a "material fact represented in the certificate is false," a material prerequisite to the certificate's issuance was missing, or the certification authority's private key or trustworthy system was compromised in such a way that the certificate's reliability is in question.[183] Regardless of the circumstances surrounding a certificate's suspension or revocation, a certification authority must "publish notice of the suspension or the revocation if the certificate was published, and otherwise must disclose the fact of suspension or revocation on inquiry by a relying party."[184] Thus, the certification authority's services toward the subscriber continue indefinitely, as does the duty owed.

Even when the relationship is ending, certification authorities, like attorneys, are limited to the manner in which they may discontinue their services.[185] Before discontinuing, a certification authority must: (1) review all the valid certificates it has issued and notify subscribers listed in those certificates; (2) do so in such a manner that disruption to subscribers and relying parties is minimized; and (3) make arrangements to preserve the certification authority's records.[186] These duties bear striking similarities to the fiduciary duties imposed upon attorneys.[187] While the ABA Digital Signature Guidelines explicitly reject a fiduciary duty of care toward the subscriber,[188] the certification authority's obligations suggest otherwise.[189]

---

181. Fisher, *supra*, note 180, at 12.

182. *Digital Signature Guidelines, supra* note 95, § 3.11.

183. *Id.* The certification authority must promptly notify the subscriber after such suspension or revocation. *Id.*

184. *Id.* § 3.12.

185. *Id.* § 3.13.

186. *Id.*

187. *See* ABA MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.16 (1983) (restricting attorneys from withdrawing from a matter where it has a "material adverse effect on the interests of the client . . . .").

188. *See Digital Signature Guidelines, supra* note 95, § 2.4 ("A certification authority is a fiduciary to a subscriber where a certification authority holds that subscriber's key or where provided by contract. A certification is not otherwise a fiduciary to a subscriber and is not a fiduciary to any relying party, except where provided by contract or by law.").

189. It is somewhat paradoxical that a certification authorities' duties rival those of an attorney, yet under the A.B.A. guidelines, should not be regarded as a fiduciary.

The greatest concern the authors have about the constant refrain expressed touting the similarities of notaries and certification authorities is that it will become a self-fulfilling prophecy. That would be tragic. There are far too many notaries—about 4.2 million of them.[190] As they have proliferated in number, they have diminished in stature and respect.[191] The Supreme Court observed that "the significance of the position [of notary public] has necessarily been diluted by changes in the appointment process and by the wholesale proliferation of notaries."[192] This overpopulation problem cannot be allowed to develop for certification authorities, for it is the most serious fault of the present notary public system in this country.

There are no substantial general education requirements for notaries.[193] But, lawyers, certified public accountants, dentists, doctors, schoolteachers, and other professionals must fulfill minimum general education requirements—such as obtaining a college degree.[194] Individuals acting as certification authorities should be required to satisfy a substantial general education requirement.[195] Unfortunately, notaries are only rarely required to undergo specialty training or testing in notarial practice, ethics and law.[196] But, many other professionals must satisfy significant specialized educational and testing requirements—such as those demanded of public school teachers, medical doctors, attorneys, certified public accountants, and real estate brokers.[197] Certification au-

190. *See The 1997 NNA Notary Census*, NAT'L NOTARY, May 1997, at 30 (reporting the total of United States notaries in 1997 to be 4,290,634).

191. Closen, *supra* note 59, at A23.

192. Bernal v. Fainter, 467 U.S. 216, 223 (1984).

193. Closen, *supra* note 59, at A23.

194. *See, e.g.*, 105 ILL. COMP. STAT. 5/21-5b (1998) (requiring a candidate for an alternative certification as a public school teacher to hold a bachelor's degree).

195. *See* Michael L. Closen & R. Jason Richards, *Cyberbusiness Need Supernotaries*, NAT'L L. J., Aug. 25, 1997, at A19 (Certification authorities "will necessarily possess significant economic power, and that is an unsettling prospect, given the historic underqualification of notaries in this country.").

196. See Closen, *supra* note 59, at A23 (pointing out that few states "require a specific level of general education" for notaries). As indicated, only a few states require training for notaries, and those requirements are either minimal or apply only in certain situations, or both: Kentucky (exam for non-attorneys only), New York (exam for non-attorney notaries only), North Carolina (must complete a community college course), Ohio (judge may require an exam), and Wyoming (exam encouraged but not required). *See also* John T. Henderson and Peter D. Kovach, *Administrative Agency Oversight of Notarial Practice*, 31 J. MARSHALL L. REV. 857, 865 (1998) ("To the extent . . . that most states do not require notary education or testing most notaries public are forced to rely upon themselves to learn how to properly exercise their commissions.").

197. For example, in Illinois, there is an alternative certification process for public school teachers requiring candidates to undergo an intensive an intensive course of study and testing on basic skills and subject matter knowledge. *See* 105 ILL. COMP. STAT. 5/21-5b (1998).

thorities should be added to that list.[198]

Many notaries public are unaware of their legal and ethical responsibilities.[199] Moreover, notaries have little financial incentive to learn. Most states strictly regulate the amount of fees that may be charged for notarial services.[200] Notaries who earn a mere $2 on average per notarization may have little motivation to learn to follow their legal obligations.[201] This in turn leads to further trivialization of the notary, as well as increased incidents of notarial fraud.[202] Notwithstanding the paramount importance of a notary's services to commerce and society, in the United States the role of notary public is deemed "essentially clerical and ministerial."[203] In contrast, notaries in other countries are held in great esteem as legal professionals, charging substantial fees and bearing significant responsibilities.[204] In Mexico, the "latin notariate" enjoys favorable social status and commands a high income.[205] The latin notariate is considered a public officer after a long period of professional preparation.[206] Japanese notaries also command handsome fees, sometimes in excess of $500, while their American counterparts are often paid a paltry $1 or $2.[207] Notaries in England also charge substantially more than the American notary, sometimes as much as $250 for a signature

198. Closen & Richards, *supra* note 195, at A19 ("It would make sense for states to develop a uniform standard exam [for certification authorities] much like the multi-state bar exam or uniform CPA exam, to insure a level of competency."). Paralegals may become the next business group to become licensed or regulated. *See Paralegal Guidelines Suggested: First In Country To Be Licensed?*, NOTARY BULL., Dec. 1998, at 13 (describing the effort in New Jersey to consider the matter and to issue a 100+ page report recommending a program of study and licensure for paralegals).

199. Closen & Richards, *supra* note 195, at A19.

200. Closen, *supra* note 59, at A23.

201. *See id.*

202. *See id; see also* Closen, *supra* note 59, at A23 ("Notary-related dishonesty appears to be on the rise.").

203. Bernal v. Fainter, 467 U.S. 216, 217 (1984). *See supra* notes 190-198 and text, for further discussion on the lack of respect and importance placed on American notaries public.

204. NOTARY LAW & PRACTICE, supra note 63, at 417. "Now, the [foreign] civil law Notary is as different from the U.S. common law Notary as an emergency medical technician is from a neurosurgeon. Where one [the foreign civil law notary] has achieved years of specialized education and training, the other [the ordinary U.S. notary] possesses a more modest, but no less important proficiency." Deborah M. Thaw, *Notaries Everywhere Share the Same Essential Values,* NAT'L NOTARY, Jan. 1999, at 5.

205. Guillermo Floris Margadant, *The Mexican Notariate*, 6 CAL. W. L. REV. 218 (1970), *reprinted in* NOTARY LAW & PRACTICE, supra note 63, at 418.

206. *Id.*

207. Thomas W. Tobin, *The Execution "Under Oath" of U.S. Litigation Documents: Must Signatures Be Authenticated?*, JAPANESE INSURANCE NEWS, July/Aug. 1995, at 34, *reprinted in* NOTARY LAW & PRACTICE, supra note 63, at 418-19.

authentication.[208] Only a handful of "notaires" are appointed in France, while there only around 1000 "notaris" in the Netherlands.[209] The Dutch notaris essentially act as attorneys, undertaking such tasks as drafting wills and contracts or setting up corporations.[210] Unfortunately, these foreign notary-professionals view our notarial system as a joke when it comes to international transactions.[211] In several countries, foreign business people "rarely take American notarizations seriously, and sometimes reject them."[212] While digital signature legislation does not presently restrict fees for an electronic certification, such fees should at least be high enough to encourage certification authorities to learn and abide by their legal obligations.[213]

A significant impediment to the position and prestige of notaries in this country[214] is the almost complete lack of financial accountability required of them.[215] Although some thirty states require each notary to be bonded, the bond levels (ranging between $500 and $15,000) are nominal and inadequate in today's economy.[216] About twenty of those thirty

208. *Id.*

209. Rene W. Clumpkens, *The Role of the Notary Under the Laws of the Netherlands, With Respect to the Transfer of Title and Encumbrance of Registered Aircraft*, 17 AIR AND SPACE LAW, at 118 (1992), *reprinted in* NOTARY LAW & PRACTICE, supra note 63, at 419-20.

210. *Id.*

211. Closen, *supra* note 59, at A24.

212. *Id.*

213. By contrast, notaries are paid nominal amounts for their services, which practice necessarily suggests a lack of importance of those services. *See* Closen, *supra* note 59, at A23.

214. The concern about the adequacy (or inadequacy) of notary bonds is almost uniquely an issue for this country because notaries in so many other countries are full legal professionals—often lawyers as well as notaries. *See* Closen, *supra* note 61, at 699 (discussing Central and South American, French, and Japanese notaries).

215. *See* Closen, *supra* note 59, at A23 (arguing that the required notary bond amounts are so low as to be "useless and misleading"); Closen & Dixon, *supra* note 45, at 893 (stating that "[t]he notarial bond will do little to protect the notary").

216. Michael J. Osty, *Notary Bonds and Insurance: Increasing the Protection for Consumers and Notaries*, 31 J. MARSHALL L. REV. 839, 845-46 & n.30. State bond requirements vary considerably. *See* ALA CODE. § 36-20-3 (1991) ($10,000); ALASKA STAT. § 44.50.120 (Michie 1989) ($1,000); ARIZ. REV. STAT. § 41-315 (1992 & Supp. 1995) ($5,000); ARK. CODE ANN. § 21-14- 101(d)(1) (Michie 1996) ($4,000); CAL GOV'T CODE. § 8212 (West 1992 & Supp. 1996) ($15,000); D.C. CODE ANN. § 1-803 (1992) ($2,000); FLA. STAT. ANN. § 117.01(4) (West 1996) ($5,000); HAW. REV. STAT. § 456-5 (1995) ($1,000); IDAHO CODE § 51-105(2) (1994) ($10,000); 5 ILL. COMP. STAT. 312/2-105 (West 1993 & Supp. 1996) ($5,000); Ind. Code Ann. § 33-16-2-1(c) (West 1992 & Supp. 1996) ($5,000); KAN. STAT. ANN. § 53-102 (West 1983) ($7,500); KY. REV. STAT. ANN. §§ 423.010-.990 (Michie 1992) (ranging usually from $500 to $1,000 depending upon the county); LA. REV. STAT. ANN. § 35:1 (West 1985 & Supp. 1996) ($5,000); MICH. COMP. LAWS ANN. § 55-110 (West 1991) ($10,000); MISS. CODE ANN. § 25-33-1 (1991) ($5,000); MO. ANN. STAT. § 486-235 (West & Supp. 1996) ($10,000); MONT. CODE ANN. § 1-5-405 (1995) ($5,000); NEB. REV. STAT. § 64-102 (1990) ($10,000); NEV. REV. STAT. ANN. § 240.030 (Michie 1996) ($10,000); N.M. STAT. ANN. § 14-12-3 (Michie 1995) ($500);

states set notary bond levels between $1000 and $5000.[217] The other twenty states do not require any surety bond at all for notaries,[218] and no state requires notaries to be covered by errors and omissions insurance.[219] The result is that users of notarial services are not statutorily protected in realistic ways against negligent and intentional misconduct by notaries,[220] because the financial injuries caused by notarial malpractice can readily exceed the trivial notary bond levels.[221] While other professionals, such as doctors, lawyers, and accountants, are not required to carry bonds or insurance, the system of protection of their consumers against malpractice tends to work because those professionals ordinarily carry adequate insurance and/or possess sufficient assets to pay claims against them.[222] Of course, bond and even insurance coverage can be required by statute,[223] as mandatory automobile liability insurance illustrates.[224] Certification authorities should be required to have minimum (though substantial) levels of bond and insurance coverage in order to adequately protect against both intentional and negligent misconduct.[225] Additionally, the statutes should provide that the amount of

---

N.D. CENT. CODE § 44-06-03 (1993) ($7,500); OKLA. STAT. ANN. tit. 49, § 2 (West 1988 & Supp. 1996) ($1,000); 57 PA. CONS. STAT. ANN. § 154 (1996) ($3,000); S.D. CODIFIED LAWS § 18-1-2 (Michie 1995) ($500); TENN. CODE ANN. § 8-16-104 (1993) ($10,000); TEX. GOV'T CODE ANN § 406.010 (WEST 1990) ($2,500); UTAH CODE ANN. § 46-1-4 (1993) ($5,000); WASH. REV. CODE ANN. § 42.44.020 (West 1991) ($10,000); WIS. STAT. ANN. § 137.01 (West 1989) ($500); WYO. STAT. ANN. § 32-1-104 (Michie 1996) ($500).

217. Osty, *supra* note 216, at 845 n.30.

218. *Id.* at 851-55 (calling for states to require errors and omissions insurance for notaries).

219. *Id.*

220. *Id.*

221. *Id.*

222. Most notaries public on the other hand tend not to be highly paid professionals, but rather work in businesses other than the provision of notarial services. Most notaries work as bank tellers, secretaries, sales persons, paralegals, clerks, and the like—positions in which the notarial function occupies only a small part of the job description. *See* Closen, *supra* note 61, at 662 ("Unlike most other public officials, notaries do not serve full-time in their official capacity. It is a sideline to their principal positions.").

223. *See, e.g.*, Shavers v. Attorney General, 267 N.W.2d 72, 77-79 (Mich. 1978) (finding state imposed insurance requirement constitutional); Rybeck v. Rybeck, 358 A.2d 828 (N.J. 1976); Andrew v. State, 233 S.E.2d 209 (Ga. 1977) (holding that mandatory insurance does not violate an individual's rights).

224. *See* Michael L. Closen & Michael J. Osty, *Illinois' Million-Dollar Notary Bond Deception*, CHI. DAILY L. BULL., Mar. 2, 1995, at 6 (pointing out that about 30 states require notaries to be bonded); Osty, *supra* note 216, at 845-846.

225. *See Digital Signature Guidelines*, *supra* note 95, § 3.3 & cmt. 3.3.3 ("Financial responsibility may be assured through security arrangements such as surety bonds or standby letters of credit, or perhaps through liability insurance . . . ."). *Id.* For further discussion of certification authority liability, *see* MICHAEL S. BAUM, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY: LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES (1994). *See also* Closen & Richards, *supra* note 4, at 747-748 (sug-

bond and insurance protection must be disclosed in each certification authority's repository, and that a certification authority may not verify a document or instrument declaring a face value exceeding the bond or insurance coverage of the certification authority.

It has been argued that a notary acts as a fiduciary to those who use the notary's services, although this viewpoint is not shared universally.[226] Yet, as noted earlier, the certification authority is generally not considered a fiduciary to a subscriber[227] and must conform only to a standard of ordinary care,[228] in spite of the fact that digital signature legislation requires the certification authority to have higher qualifications, training and expertise than the notary, as well as greater responsibilities.[229] We believe that digital signature legislation must impose substantial responsibilities on all of the parties to electronic transactions. Holders of private keys should have absolute liability for the use (authorized or otherwise) of the private key.[230] Recipients of electronic documents should be entitled to reasonably rely upon them only after thorough review of both the certificate of authentication for the document and the repository information of the certification authority (including the CRL), and only to the extent of the financial responsibility for which the certification authority is accountable.[231] The certification authority must be declared to be a fiduciary of all of its electronic commerce clients, senders and recipients alike,[232] thus, imposing a higher set of

---

gesting that the financial accountability of certification authorities be thoroughly considered and that legislation establish substantial bond and/or insurance requirements for them).

226. Closen, *supra* note 61, at 662-65.

227. *Digital Signature Guidelines*, *supra* note 95, § 2.4 ("A certification authority is a fiduciary to a subscriber where a certification authority holds that subscriber's key or where provided by contract. A certification is not otherwise a fiduciary to a subscriber and is not a fiduciary to any relying party, except where provided by contract or by law"). *Digital Signature Guidelines*, *supra* note 95 § 2.4, cmt. 2.4.1 further provides that "[a] certification authority typically provides services at arm's length and does not create a special relationship with its subscribers or relying parties, such as a fiduciary relationship." *Id.*

228. *See id.* cmt. 2.3.4 ("A certification authority is charged with treating its subscribers and others with ordinary care . . . .").

229. *See also Digital Signature Guidelines*, *supra* note 95, § 1.6, cmt. 1.6.3 (Stating that a Cybernotary must posses "technical expertise to facilitate computer-based transactions requiring a high level of certification . . . .") *Id.*

230. *But see Digital Signature Guidelines*, *supra* note 95, § 4.3 cmt. 4.3.2 ("This Guideline is intentionally silent about the precise standard of care applicable to a subscriber's duty not to divulge the private key.").

231. *See Digital Signature Guidelines*, *supra* note 95, § 5.4 (discussing factors that may lead to reasonable reliance upon a certificate).

232. *But see Digital Signature Guidelines*, *supra* note 95, § 2.4 ("A certification authority is a fiduciary to a subscriber where a certification authority holds that subscriber's private key or where provided by contract. A certification authority is not otherwise a fiduciary to a subscriber [or a] relying party, except where provided by contract or by law.")

duties than the ordinary duty of reasonable care. This issue is particularly critical when one considers the enormous volume of substantial commercial transactions that are conducted over the Internet on a daily basis, and that this volume will continue to rise at a rate that is truly inestimable.[233]

Only a handful of states require criminal background checks before a notary may be commissioned.[234] In contrast, the Latin Notariate must have "good moral character," and a criminal record free of dishonorable acts.[235] The Washington Digital Signature Statute for certification authorities also sets forth very strict guidelines in this respect.[236] It requires firms serving as certification authorities to refrain from employing any person convicted of a felony in the past fifteen years, and restricts certification authorities from employing anyone ever convicted of a crime involving fraud, false statement, or deception.[237] The Act further requires that certification authorities only employ persons with a demonstrated knowledge of the Act's provisions.[238] Utah's Digital Signature Act has similar background provisions and goes further, eliminating the "past fifteen years" language, thereby, prohibiting certification authorities from employing anyone convicted of a felony or crime involving fraud, false statement or deception.[239]

The most critical part of the certification authority's task is to verify the identity of the parties to the transaction. Washington's Act requires certification authorities to confirm that: (1) the subscriber is indeed the person listed in the certificate to be issued or a duly authorized agent; (2) the information in the certificate is accurate; (3) the prospective sub-

---

Id; *see also* cmt. 2.4.1 ("A certification authority typically provides services at arm's length and does not create a special trusted relationship with its subscribers or relying parties, such as a fiduciary relationship.") *Id*. *But see* cmt. 2.4.3 ("The commercial marketplace and usage of trade will ultimately determine the extent of any demand for "fiduciary-like" certification services.") *Id*.

233. *See supra* notes 9-10 and 14-15 and accompanying text, and *infra* note 254.

234. Henderson & Kovach, *supra* note 196, at 865. Only Massachusetts, Missouri, Minnesota, New Hampshire, and New York require law enforcement officials to perform such procedures. *Id*.

235. Pedro A. Malavet, *The Foreign Notarial Legal Services Monopoly: Why Should We Care?*, 31 J. MARSHALL L. REV 945, 964 (1998).

236. *See* WASH. REV. CODE ANN. § 19.34.100 (Supp. 1998). By comparison, Washington's notary qualifications are fairly lenient, requiring only that a notary be at least eighteen years old, read and write English, and either reside, work or do business in the state. *Id*. § 42.44.020.

237. *See id*.

238. *See id*.

239. UTAH CODE ANN. § 46-3-201 (Supp. 1996). By comparison, Utah's notary statute requires only that a notary be at least eighteen years old, a resident of the state for thirty days, able to read, write and understand English, and a statement of personal information. *Id*. § 46-1-3.

scriber holds the appropriate corresponding private key; and (4) the certificate contains sufficient information to locate a repository in case the certificate is suspended or revoked.[240] Both the Washington and Utah statutes provide that by issuing certificates, certification authorities warrant that the certificates contain no information known to be false, were issued within the certification authority's authority, and satisfy the other requirements of each respective act.[241] Sadly, like most notary statutes, neither state provides specific guidelines for identifying the parties to a reasonable degree.[242] While identification guidelines in digital signature legislation are lacking, current laws require a fairly comprehensive record keeping system.[243] The A.B.A. Digital Signature Guidelines require that a certification authority "document all facts material to the issuance, suspension, or revocation by it of a certificate, and retain that documentation for an appropriate time."[244] The comments to this section suggest that records "could include" information relating to the parties' identification, but unfortunately make no specific requirement.[245] In contrast, notarial acts performed in civil jurisdictions are officially considered public documents, regardless of whether they are of a public or private nature.[246] Several states even require that ordinary notaries public maintain a notary log or journal that must include several items of information such as the name and address of the document signer, the signature of the document signer, and the method of identifying the document signer (with supporting detail).[247] California also requires the document signer to place his/her right thumbprint in the

240. WASH. REV. CODE ANN. § 19.34.210 (Supp. 1998). This provision also prohibits waiver of these requirements by either party. *See id.*

241. *See id.* § 19.34.220 and UTAH CODE ANN. § 46-3-303 (Supp. 1996). These provisions also prohibit waiver of these requirements by either party.

242. Most states do not provide specific guidelines for identifying parties. However, a few states require that the notary maintain a journal that identifies each notarization. *See, e.g.*, CAL. GOV'T § 8206 (West 1992) (requiring notary to record date, time and type of each notarization, character of the document notarized, the signature and manner of identification of each party, and a fingerprint where the notarization involves transfers of land interests). For further discussion of the favorability of thumbprinting, see *Thumbprinting: "The Notary's Best Anti-Fraud Weapon,"* NOTARY BULL., June 1995, at 1, 13.

243. Similarly, states may require notaries to keep such records. *See* UTAH CODE ANN. § 46-1-15 (stating that if a notary keeps a journal record, it must be safeguarded as a valuable public document and kept in the exclusive custody of the notary).

244. *Digital Signature Guidelines*, *supra* note 95, § 3.5.

245. *Id.* at cmt. 3.5.1.

246. Malavet, *supra* note 235, at 955 & n.39, (*citing* France (C. CIV., ARTS. 1317, 1319; ORDINANCE No. 45-2590 of 2.11.1945, ART 1; LAW OF 25 VENTOSE YEAR XI, ART. 19)); Belgium (CIV. CODE ARTS. 1317, 1319; LAW OF 25 VENTOSE YEAR XI, ARTS. 1, 19); Italy (C.C. ARTS. 2699, 2700; NOTARIAL LAW (1913), ART. 1); Spain (C.C. ARTS. 1216, 1218; CIV. PROCEDURE LAW, ART. 596; NOTARIAL LAW (1862), ART. 1; NOTARIAL REGULATIONS (1944), ARTS. 1, 2); Germany (ZPO, ARTS. 415(1), 418(1), 437, NOTARIAL ORDINANCE (1961), ART. 1).

247. Van Alstyne, *supra* note 72, at 778 & n.5.

notary journal for certain real estate documents.[248]

Market forces alone may not be enough to assure that only a small number of well-qualified entities (and the people behind them) become licensed as certification authorities. State legislation should strictly regulate the number of entities offering certification authority services, while reserving the "root certification authority" for a government entity, such as the Secretary of State.[249] Limitations on the number of licensed certification authorities may be based on the total population, or on the volume of business transactions conducted. But, we urge that governments err on the side of too few licenses, for the numbers can always be increased as commercial need warrants. Alternatively, similar federal statutes and regulations may be more appropriate to ensure that the certification authority's role in electronic commerce will receive the paramount and uniform national attention that it deserves.[250] Under this scheme, an agency such as the Federal Trade Commission might serve as the "root authority," allowing individual state secretaries of state to serve as a secondary root authority. Increased uniformity of practice within the United States along with its encouragement of growth of electronic business would be among the important advantages to be gained from these legislative steps.[251] These steps would also help ensure that

248. Gnoffo, *supra* note 42, at 805 & n.19 (citing CAL. GOV'T CODE § 8206(a)(7)) (West 1992 & Supp. 1996).

249. *See* Closen & Richards, *supra* note 195, at A19 (observing that certification authorities "will necessarily possess significant economic power, and that is an unsettling prospect, given the historic underqualification of notaries in this county;") *See also supra* notes 139-143 and accompanying text.

250. *See* Hill, *supra* note 4, at 12 ("Congress has not yet enacted any federal law governing digital signatures and electronic commerce, although the banking lobbyists have been anxious to have it do so."); Newcombe, *supra* note 58, at 44 ("Fearing a litany of state laws may stifle electronic commerce, a number of firms and business groups have pressured Congress to establish sweeping national laws governing electronic authentication—an important tool for safe and secure transactions on the Internet.") *Id.*

251. *See* Newcombe, *supra* note 58, at 44. ("[S]oftware firms that make authentication tools and the firms that would use them made it clear they believed states are moving too slowly on the issue of legalizing electronic authentication and are producing legislation loaded with conflicting regulations that might prove too burdensome for electronic commerce to flourish.") *Id*; ("There is concern that nonuniform state laws may have a negative effect on the development of electronic banking and commerce.") Hill, *supra* note 4, at 12; ("Ideally, Congress should address [heightened standards for certification authorities] as a national issue, but the current states' rights climate and the traditional lack of federal interest in notaries makes this unlikely, so the matter rests with the states.") Closen & Richards, *supra* note 195, at A19. However, there is also a point of view favoring state regulation of electronic commerce. Newcombe, *supra* note 58, at 44.

> In explaining why it favors a state-led approach to developing digital signature policies and standards, the American Bar Association pointed out that premature legislation at the national level 'runs the risk of stunting the natural evolution of market forces that will produce the most cost-efficient, user-friendly, interoperable and effective implementation of digital signatures. While early adopters of digital

electronic documents authenticated by American companies will be acceptable to foreign business people, unlike some of the paper documents authenticated by American notaries public.[252]

V. CONCLUSION

> "There is no reason for any individual to have a computer in their home."[253]
>
> Ken Olson, President, Chairman, and founder of Digital Equipment Corp., 1977.
>
> "The numbers are already staggering, but they'll explode over the next five years—28.7 million computer users in the United States in 1998, 45.3 million by the millennium and a mind-boggling 77.6 million by the year 2002."[254]
>
> Janet Key, for the American Bar Association Journal, 1998.

The United States Treasury Department's Office of the Comptroller of Currency recently declared a certification authority to be the "functional equivalent" of a notary.[255] The authors are quite bothered by comparisons of that kind. It is probably more accurate to say that a certification authority or cybernotary resembles an enhanced or "hybrid"

---

signature technology desire greater national uniformity in the immediate future, the overall interests of evolving the best public-key infrastructure requires a period of experimentation.

Id.

252. Closen & Richards, *supra* note 195. "Since notaries are esteemed in many other countries and used regularly by business professionals, [the] debasement of the office [of notary public] in America is likely to become a problem for international [electronic] commerce, particularly as more and more arrangements and agreements are made in cyberspace." *Id.* "It is becoming increasingly important to have reliable, reputable certification authorities that are recognized worldwide, in order to ensure secure global transactions like those used in international banking." Hill, *supra* note 4, at 11. *See supra*, notes 190-213 and supporting text for further discussion of the lack of respect given to American notaries and the documents they notarize.

253. Closen, *supra* note 195.

254. Janet Key, *Spin Your Own Web*, A.B.A. J., Nov. 1998, at 76; *see also Internet Traffic Booming*, DAILY SOUTHTOWN [AP], Apr. 16, 1998, at 1 ("Traffic on the Internet is doubling every 100 days, the government said Wednesday in the latest snapshot of the exploding information technology industry.") *Id.*

255. *See* letter from Julie C. Williams, Chief Counsel, Controller of the Currency, Administrator of Banks, to Stanley F. Farrar, Esq., Sullivan & Cromwell, Jan. 12, 1998 (visited August 19, 1998) <http://www.occ.treas.gov/ftp/release/98-4att.pdf>. *See also* Philip S. Corwin, *Notaries in Cyberspace: A New Role for Banks*, AM. BANKER, Feb. 10, 1998, at 4, *available in* 1998 WL 4880265 (discussing Office of Comptroller's determination that Certification Authorities are the functional equivalent of a notary, and, therefore, allowed a national bank to establish a certification authority service); *see also Digital Signature Guidelines*, *supra* note 95, § 1.6, cmt. 1.6.3 (determining that the Cybernotary's function mirrors that of a notary).

notary.[256] While serving the same document signer identification function as notaries, certification authorities also verify the integrity of the substance of the documents to which the parties bind themselves.[257] That constitutes an enormously important distinction between the two posts. Moreover, both the potential volume and magnitude of transactions with which certification authorities will be called upon to deal greatly distinguish the post from the relatively insignificant notary public. The estimates revealed in Janet Key's statement (as quoted just above[258]) confirm our point. Unfortunately, due to the trivialized nature of the traditional notary public, the certification authority may face a similar fate.

The "staggering" growth predicted will not be without its complications. Some claim that digital signatures verified by certification authorities are impregnable. "It is mathematically impossible to forge someone else's digital signature."[259] But, others caution that "no security scheme is 100% unbreakable."[260] Indeed, inherent in such fast-paced expansion of technology is the risk of mistakes, abuses, and frauds occurring.[261]

Every system is subject to the factor of human involvement. And, human error, including flawed judgment, is an ever-present prospect. First of all, the private key can assure secure communication only if it is kept truly private by the people who control it. In October of 1998, LEXIS-NEXIS dispatched an "Urgent Security Notice" to law schools warn-

256. *Certification Authorities Add Another Layer of Security*, HEALTH DATA MGMT., Sept. 19, 1997, *available in* 1997 WL 8747997. "A certification authority is similar to a notary public, only more complete." *Id.*

257. Elliott, *supra* note 65, at 915.

258. Key, *supra* note 254, at 76.

259. Klau, *supra* note 6, at 14.

260. See internet site <http://www.internic.net/faq/guardian.html>.

261. Regarding the possibility of serious mistakes occurring, many computer software programs seem to be plagued by glitches or bugs. *See, e.g.*, Becky Beaupre, *Computer Glitch at 24 Libraries Is One for the Books*, CHI. SUN-TIMES, May 6, 1998, at 34 (reporting that 24 suburban libraries encountered a computer glitch lasting eight days and denying the libraries the ability to determine whether books were checked out without physically going to the shelves); *Computer Glitch Gives Retirees Extra Social Security Interest,* Chicago Tribune, Dec. 22, 1998, Section 1 at 25 (reporting that a "computer glitch has resulted in Social Security's reserve account earning higher interest than it should," the total amount estimated to be about $4.4 billion). Of course, the major problem that just about everyone seems to be talking about is the Y2K millennium bug. There have been countless articles addressing this concern. *See, e.g.*, Howard Wolinsky, *Y2K Glitch Could Rear Its Head This Week*, CHI. SUN-TIMES, Dec. 28, 1998, at 1 (discussing the prospect that serious Y2K problems could really begin at various times in 1999); Robert G. Gerber, Comment, *Computers and the Year 2000: Are You Ready?*, 30 J. MARSHALL L. REV. 837 (1997) (discussing the significance of the Y2K problem, and the issue of who ought to bear the cost for Y2K-compliance). With respect to the role of notaries in dealing with Y2K problems, see David S. Thun, *Following the Paper Trail: Notaries and the Y2K Crisis,* NAT'L NOTARY, Jan. 1999, at 18.

ing of an e-mail scam in which impostors purporting to act for LEXIS-NEXIS, "under various pretenses," requested customers to provide their LEXIS-NEXIS passwords or identifiers.[262] According to the security flyer and cover letter, some customers were duped into supplying their codes to the impostors.[263] Some law enforcement agencies have begun placing criminal "wanted" listings on-line.[264] Imagine the chaos and injury that could result from such listings being accessed and tampered with by an unauthorized high-tech hacker or intruder. There is also concern about the confidentiality of the contents of electronic communications, but sometimes the holders of information and the senders of messages simply do not take enough security steps to protect against unwanted disclosures.[265]

One consequence of the arrival of the information era is that just about everything seems to have been made available on computer databases—academic, financial, criminal, medical, and other records.[266] And, much of this information is quite sensitive and should be kept confidential. Secondly, the certification process can assure secure communication only if the people who control it remain untouched by the temptations of collusion and corruption. There is no reason to expect that the people who serve as certification authorities will rise above the same kinds of misconduct that have been committed by private individuals and public officers at every level.[267] Rigorous credentialing of certification authorities must be mandated. Otherwise, even if diamond

262. *See* Letter, from LEXIS-NEXIS, to Law School Faculty & Staff, Oct. 29, 1998 (relating to "E-mail and Telephone Scam,") with "URGENT SECURITY NOTICE" attachment ("A scam is currently being perpetrated upon a few LEXIS-NEXIS customers by both e-mail and telephone. This scam asks the customer to provide their LEXIS-NEXIS ID (code) to a generic e-mail box or over the phone.") *Id.* Copies of both the letter and attachment are on file with the authors.

263. *Id.* The attachment directed customers to report to their account representative "if you have been contacted and/or have already provided your LEXIS-NEXIS ID. . . .". The letter also suggested that some customers may have been "contacted and provided ID information" to the scam artists. *Id.*

264. *See Wanted: Listings on Web*, THE STAR [newspaper], Nov. 5, 1998, at B3 (reporting that police in Lincoln, Nebraska, have published "more than 6000 names of people who have outstanding warrants" on the Internet). *See also* <http://interlinc.ci.lincoln.ne.us>.

265. "In the pursuit of quick access to medical records, [on-line] systems are being built without any thought to privacy." Deidra Mulligan, Staff Counsel to the Center for Democracy and Technology, quoted in *Medical Records On-line For All To See?*, TRIAL, Dec. 1998, at 12.

266. For further discussion of medical records on-line and issues of confidentiality and security, see Robert O'Harrow Jr., *Plans' Access to Pharmacy Data Raises Privacy Issue*, WASH. POST, Sept. 27, 1998, at A1; *see also* Milt Fruedenheim, *Medicine at the Click of a Mouse: On-line Health Files Are Convenient. Are They Private?*, N.Y. TIMES, Aug. 12, 1998, at D1.

267. For instance, "[n]otary-related dishonesty appears to be on the rise." Closen, *supra* note 59, at A23.

dealers Carroll and Jean employed the services of a certification authority for their transaction,[268] there would be less assurance that fraud could be avoided.

Certification authorities will be asked to fill a critical role as the gatekeepers of secure communications and transactions in the information age, but their futures are at risk. Yet, at the same time, their futures could become very bright. We have the truly rare opportunity for business and legal policy to move ahead almost simultaneously with technology as it relates to the functioning of the certification authority in electronic commerce. Admittedly, developing legal and policy guidelines for technology while in its infant stages is "somewhat like trying to board a moving bus,"[269] but it must be attempted. If we delay, we will be far too late. Once the bus has left, its path will become fixed—impossible to undue the ground that has already been covered and increasingly difficult to modify even as to its more distant route ahead. Now is the only time when heightened standards for the appointment and conduct of certification authorities can effectively be implemented. Perhaps the bus has not quite left yet. As one commentator has suggested, "Digital signatures are still a solution in search of a problem . . . . People don't know what to do with [them] yet."[270]

268. *See* the hypothetical illustration that introduced this paper, *supra* notes 3-4 and accompanying text.

269. Bensusan Restaurant Corp. v. King, 126 F.3d 25, 27 (2d. Cir. 1997). "It would be easier to lasso Jell-O than to apply traditional regulatory structures to the Internet." Pearce, *supra* note 11, at 14, *quoting* Susan Ness.

270. Newcombe, *supra* note 58, at 44 (quoting Todd Sander, Deputy Director of the Washington State Department of Information Services.) Although online commerce is growing dramatically, the use of digital signature technology has not taken root so firmly yet. Commerce Secretary William M. Daley commented that "the digital economy is alive and well and growing." *Internet Traffic Booming*, DAILY SOUTHTOWN [AP], Apr. 4, 1998, at 1. "The information technology industry is growing as fast as the overall economy." *Id.* at 2. However, "[a]lmost no cybernotaries have been appointed or have yet begun to function." Closen & Richards, *supra* note 4, at 715. Although Utah in 1995 became the first state to adopt digital signature and certification authority legislation, it has just begun to register certification authorities. *See First 'Certification Authorities' May Register Electronic Notaries*, NOTARY BULL., Feb. 1999, at 9.