UIC John Marshall Journal of Information Technology & Privacy Law

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

Article 6

Spring 1999

The Utah Digital Signature Act As "Model" Legislation: A Critical Analysis, 17 J. Marshall J. Computer & Info. L. 873 (1999)

R. Jason Richards

THE UTAH DIGITAL SIGNATURE ACT AS "MODEL" LEGISLATION: A CRITICAL ANALYSIS

by R. JASON RICHARDS†

I. INTRODUCTION

It has been suggested that the Internet[1] is "the most profound transformation a technology has brought since the capture of fire."[2] This statement may not be too far from the truth. In simpler days, business transactions consisted of nothing more than a pen, paper, and face-to-face contact.[3] The Internet has changed all that. Today, parties are just as likely to communicate in the new and sophisticated world of "cyberspace" than in any other medium, thereby "replacing physical interaction with virtual communications,"[4] and, in the process, creating opportuni-

† B.A., B.A., University of Alabama at Birmingham; J.D., The John Marshall Law School; LL.M. candidate, DePaul University College of Law.

1. The term "Internet" is defined as "a set of computer networks—possibly dissimilar—joined together by means of gateways that handle data transfer and the conversion of messages from the standing network to the protocols used by the receiving network." MICROSOFT PRESS COMPUTER DICTIONARY 220 (2d ed. 1994).

2. *Internet Symposium: Legal Potholes Along The Information Superhighway,* 16 LOY. L.A. ENT. L.J. 541, 601 (1996).

3. Diana J.P. McKenzie, *Commerce on the Net: Surfing Through Cyberspace Without Getting Wet,* 14 J. MARSHALL J. COMPUTER & INFO. L. 247, 247 (1996).

4. Daniel V. Logue, Note, *If the International Shoe Fits, Wear It: Applying Traditional Personal Jurisdiction Analysis to Cyberspace in* Compuserve, Inc. v. Patterson, 42 VILL. L. REV. 1213, 1213 (1997). Current figures put the number of Internet users in the United States and Canada alone at 58 million. G. Christian Hill, *Adult Users of the Net in U.S. and Canada Put at 58 Million,* WALL ST. J., Dec. 11, 1997, at *1.

While the prospect of a purely paperless society is intriguing, it is unlikely that this ideal will ever come to fruition. First, paper has an unparalleled record of superiority when it comes to long-term storage. *See* Michael L. Closen & R. Jason Richards, *Notaries Public—Lost in Cyberspace, Or Key Business Professionals of the Future?,* 15 J. MARSHALL J. COMPUTER & INFO. L. 703, 715 (1997) [hereinafter Closen & Richards, *Lost in Cyberspace*]. Second, "as crude as it may be, a piece of paper . . . enjoys many security advantages over a document on a computer's hard disk." MICHAEL L. CLOSEN ET AL., NOTARY LAW AND PRACTICE: CASES AND MATERIALS 35 (1997) [hereinafter NOTARY LAW] (quoting Charles N. Faerber, *The Notary and EDI,* Paper presented to Work Group on Notarization and Nonrepudiation, ABA Information Security Comm., Jan. 10, 1993). Third, the sophisti-

ties for electronic commerce that were unimaginable not too long ago.[5]

Not surprisingly, much has been written about the many new legal issues this emerging commercial forum presents.[6] One aspect of electronic commerce that has received considerable scholarly and legislative

---

cated nature of electronic communications may alienate potential users, meaning that "[s]ome people will not learn the technology[,] [s]ome will not be able to afford the technology[,] and [s]ome will not trust in the technology or those who control it." Closen & Richards, *Lost in Cyberspace*, *supra*, at 715. Finally, paper records will likely survive into the future because "[s]ome documents, like original, recorded deeds . . ., should not be destroyed even if digital backup files exist." Paul Berstein, *The Paperless Desktop—A Virtual Reality?*, TRIAL, Mar. 1997, at 54, 57.

5. *See* Daniel J. Greenwood & Ray A. Campbell, *Electronic Commerce Legislation: From Written on Paper and Signed in Ink to Electronic Records and Online Authentification*, 53 BUS. LAW. 307, 307 (1997); *see also* R. J. Robertson, *Electronic Commerce on the Internet and the Statute of Frauds*, 49 S.C. L. REV. 787, 824 (1998) (noting that "technological developments have brought about a revolution in communication and business practices, centering on the use of personal computers connected through a web of networks commonly known as the 'Internet.'"); William E. Wyrough Jr. & Ron Klien, *The Electronic Signature Act of 1996: Breaking Down Barriers to Widespread Electronic Commerce in Florida*, 24 FLA. ST. U. L. REV. 407, 414 (1997) ("Society is rapidly advancing forward to a day when information technologies will be an integral part of daily life.").

6. A small sample of the many legal issues cyberspace has presented include:
Jurisdiction. See, e.g., John Gilbert, *Questions of Authority: Jurisdiction Cases Crop Up As Internet Sales Erase Borders*, 83 A.B.A. J. 42, June 1992; Craig P. Gaumer, *The Minimum Cyber-Contacts Test: An Emerging Standard of Constitutional Personal Jurisdiction*, 85 ILL. B.J. 58 (1997); Todd H. Flaming, *The Rules of Cyberspace: Informal Law in a New Jurisdiction*, 174 ILL. B.J. 85 (1997); Juan Andres Avellan V., *John Hancock in Borderless Cyberspace: The Cross-Jurisdictional Validity of Electronic Signatures and Certificates in Recent Legislative Texts*, 38 JURIMETRICS J. 301 (1998); David L. Stott, *Personal Jurisdiction in Cyberspace: The Constitutional Boundary of Minimum Contacts Limited To a Web Site*, 15 J. MARSHALL J. COMPUTER & INFO. L. 819 (1997); Richard S. Zembeck, *Jurisdiction and the Internet, Fundamental Fairness in the Networked World of Cyberspace*, 6 ALB. L. J. SCI. & TECH. 339 (1996); Martin F. Noonan, *Civil Procedure—Personal Jurisdiction: Evolving Current Interpretation of the Stream of Commerce Test in the Third Circuit*, 40 VILL. L. REV. 779 (1995). *See generally* M. Ethan Katsh, *Dispute Resolution in Cyberspace*, 28 CONN. L. REV. 953 (1996). *See, e.g.*, Edward Geller, *Conflicts of Law in Cyberspace: Rethinking International Copyright in a Digitally Networked World*, 20 COLUM-VLA J. L. & ARTS 571 (1996); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993-1051-53 (1994).
The First Amendment. See generally Bruce W. Sanford & Michael J. Lorenger, *Teaching An Old Dog New Tricks: The First Amendment in an Online World*, 28 CONN. L. REV. 1137 (1996); Donald E. Lively, *The Information Superhighway: A First Amendment Roadmap*, 35 B.C. L. REV. 1067 (1994).
Antitrust law. See generally Mark Lemley, *Antitrust and the Internet Standardization Problem*, 28 CONN. L. REV. 1041 (1996).
Defamation law. See generally Robert B. Charles & Jacob H. Zamansky, *Liability for Online Libel After* Stratton Oakmont, Inc. v. Prodigy Services Co., 28 CONN. L. REV. 1173 (1996).
Obscenity Law. See generally Eric Handelman, Comment, *Obscenity and the Internet: Does the Current Obscenity Standard Provide Individuals with the Proper Constitutional Safeguards?*, 59 ALB. L. REV. 709 (1995).

attention to date involves "electronic" and "digital" signature technology.[7] The first state to address the matter was Utah, which resulted in the adoption of the Utah Digital Signature Act ("the Utah Act") in 1995. Since that time, over 35 states and jurisdictions passed some form of digital or electronic signature legislation, and most of the remaining jurisdictions are considering similar laws.[8] Of the legislation thus far enacted, most take the form of either comprehensive guidelines,[9] or very brief directives that authorize the use of electronic or digital signature technology generally.[10] Regardless of which legislative approach is adopted, however, the common thread that runs through each is that they replicate, or at least mimic, Utah's approach. What are the implications of this replication? With so many states eager to jump on the "electronic bandwagon," are states sacrificing legislative form over legislative substance? Numerous legal commentators believe so.[11] Just as the old

---

Electronic contracting. See generally Raymond T. Nimmer, *Electronic Contracting: Legal Issues*, 14 J. MARSHALL J. COMPUTER & INFO. L. 211 (1996).

Other online issues. See generally McKenzie, *supra* note 3, at 247 (addressing several legal issues relating to transacting business in cyberspace).

7. *See, e.g.*, Closen & Richards, *Lost in Cyberspace*, *supra* note 4, at 703; Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures*, J. MARSHALL J. COMPUTER & INFO. L. 189 (1997); David P. Vandagriff, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995); Wendy R. Leibowitz, *Technology and the Law Meet Online Commerce: "Digital Signature" Guidelines and an Upgraded U.C.C. Will Ease Internet Transactions, An L.A. Court Tries It Out*, 18 NAT'L L.J. 49 (1996); Gary W. Frensen, *What Lawyers Should Know About Digital Signatures*, 170 ILL. B.J. 85 (1997); Timothy Tomlinson, *Legitimizing Contracts in Cyberspace: The ABA's New Guidelines Create a Legal Infrastructure for Using Digital Signatures*, NAT'L L.J., May 5, 1997, at B11; UTAH CODE ANN. § 46-3-106 (1998) ("Utah Digital Signature Act").

8. *See, e.g.*, ARIZ. REV. STAT. ANN. §§ 41-121 (West Supp. 1997); CONN. GEN. STAT. §§ 19a-25a (1997); FLA. STAT. ANN. §§ 282.70 to 75 (West Supp. 1998); IOWA CODE § 48A.13 (Supp. 1998); LA. REV. STAT. ANN. § 40:2144 (West Supp. 1998); MINN. STAT. § 221.173 (Supp. 1998); N.M. STAT. ANN §§ 14-15-1 to 6 (Michie Supp. 1997); (UTAH CODE ANN. §§ 46-3-101 to 504 (Supp. 1997); WASH. REV. CODE ANN. §§ 19.34.010 to 903 (West Supp. 1998).

9. *See, e.g.*, UTAH CODE ANN. § 46-3-106 (1998); WASH. REV. CODE ANN. § 19.34.010 (West 1998).

10. Michael L. Closen & R. Jason Richards, *Cyberbusiness Needs Supernotaries*, NAT'L L. J., Aug. 25, 1997, at A19 [hereinafter *Supernotaries*]. *See, e.g.*, KAN STAT. ANN. § 60-2616(c) (Supp. 1997).

11. *See, e.g.*, Closen & Richards, *Lost in Cyberspace*, *supra* note 4, at 703 (discussing cybernotarial legislation and analyzing the role of such laws and the shortcomings of current and proposed legislation); Closen & Richards, *Supernotaries*, *supra* note 10, at A19 (arguing that Utah's digital signature statute, which has become the model for several states, is inadequate in many respects); Wright, *supra* note 7, at 189 (endorsing Pen Biometrics Technology ("PENOP") in lieu of Utah's public key cryptography approach); Robertson, *supra* note 5, at 824 (arguing that Utah's statute is, among other things, "too narrow because it limits electronic messages that satisfy the Statute of Frauds to those that are digitally signed"); C. Bradford Biddle, Comment, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L.

saying goes, "hard cases make bad law,"[12] so too, the author believes, do "bad [laws] bring about worse [laws]."[13] Thus, it is particularly important to expose the potential weaknesses in the Utah Act in light of its rapidly-accepted, yet troubling status as "model" legislation. Several of the Utah Act's provisions create problem areas which will only foster additional uncertainties as to how digital and electronic signature legislation and practice will work together. These uncertainties cast considerable doubts about the law's effectiveness and its rightful place in shaping both the practice and regulation of certification authorities throughout this country.[14] These problem areas are the focus of this article. However, the purpose of this article is not to discourage the evolution of digital signature or electronic signature legislation; rather, its purpose is to call attention to a variety of problematic issues found therein, for it is hoped that calling attention to the problems will help to correct the weaknesses.

This article provides a brief discussion of what a digital signature is, how it works generally, and the players involved in the process. It will then review numerous provisions of the Utah Act, including recommendations for improvements to current legislation. Finally, this article concludes that the Utah Act, while significant for the simple act of stimulating interest in electronic commerce, is not the model Act many believe it to be. The author's hope is that the suggestions offered in this article will promote remedial state action surrounding digital and electronic signature legislation.

II. ELECTRONIC SIGNATURES AND DIGITAL SIGNATURES DEFINED

There are two general categories of legislation related to electronic signatures: electronic signature legislation and digital signature legislation.[15] These two forms of legislation, while technologically distinct, are often used interchangeably, and thus, not always readily distinguishable.[16] Indeed, numerous definitions of the term "electronic signature"

REV. 1143 (1996) (discussing the misplaced priorities surrounding the allocation of liability and evidentiary burdens of Utah's law).

12. Northern Sec. Co. v. United States, 193 U.S. 197, 400 (1904) (Justice Oliver Wendell Holmes Jr. noting that "Great cases like hard cases make bad law").

13. JOHN BARTLETT, FAMILIAR QUOTATIONS 358 (15th ed. 1980) (quoting Jean Jacques Rousseau (1762)).

14. *See* Closen & Richards, *Supernotaries, supra* note 10, at A19.

15. *See* Greenwood & Campbell, *supra* note 5, at 316; *see also* Wyrough & Klein, *supra* note 5, at 424 (stating that digital signatures are a form of electronic technology).

16. *See* Theodore S. Barassi, *Electronic Signature Differs from Digital*, 214 N.Y. L.J. 102 (1995); INFORMATION SECURITY COMMITTEE, AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE 35 (1996) [hereinafter DIGITAL SIGNATURE GUIDELINES].

exist. For instance, Florida law defines electronic signature as "any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing."[17] Illinois law, on the other hand, defines electronic signature as "digital technology," noting that electronic signatures include "electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies."[18]

The primary difference between digital signatures and electronic signatures is that the digital signature approach uses a specific type of technology, while the electronic signature method does not.[19] More specifically, "digital signature" is a term usually reserved for signatures which implement public key or asymmetric cryptographic systems,[20] while "electronic signature" refers generically to any electronic technology intended by the party to validate a writing.[21] The distinction here is more than semantic; indeed, each term has independent legal significance.[22] Evidentiary proceedings, for example, favor digital signatures, whose specific, security-conscious method of identification provides proof of message integrity and non-repudiation by the document signer.[23] On the other hand, electronic signatures do not receive the same evidentiary presumption of validity because they are unverifiable and subject to both forgery and repudiation by the signer.[24] Of course, these evidentiary presumptions are subject to change depending upon the statutory makeup of the law in question.[25]

---

17. FLA. STAT. ANN. § 282.72(4) (West 1998).

18. ILLINOIS ATTORNEY GENERAL JIM RYAN'S COMMISSION ON ELECTRONIC COMMERCE AND CRIME, FINAL REPORT (May 26, 1998) [hereinafter ILLINOIS ACT]. *See also* GA. CODE ANN. § 10-12-3 (1998) ("Georgia Electronic Records and Signature Act") ("'Electronic Signature'" means an electronic or digital method executed or adopted by a party with the intent to be bound by or to authenticate a record, which is unique to the person using it, and is linked to data in such a manner that if the date are changed the electronic signature is invalidated.")

19. *See* Barassi, *supra* note 16, at 102; *Symposium: Tutorial*, 38 JURIMETRICS J. 243, 244 (1998); Maureen S. Dorney, *Doing Business on the Internet: The Law of Electronic Commerce*, 491 PLI/Pat 141, 145 (1997).

20. *Compare* UTAH CODE ANN. § 46-3-103(2) (1998) ("Utah Digital Signature Act") (implementing an the asymmetric cryptosystem) *with* GA. CODE ANN. § 10-12-3 (1998) ("Georgia Electronic Records and Signature Act") (defining electronic signature as "an electronic or digital method executed or adopted by a party with the intent to be bound by or to authenticate a record . . . .").

21. *See* Barassi, *supra* note 16, at 102; Greenwood & Campbell, *supra* note 5, at 317-18.

22. *See* Barassi, *supra* note 16, at 102.

23. *Id.*

24. *Id.*

25. *Compare* ILLINOIS ACT, *supra* note 18, § 10-110(a)(1)-(3) (establishing a rebuttable presumption that the electronic signature is of the individual to whom it correlates so long as the qualified security procedure was commercially reasonable, applied in trustworthy

Technical and evidentiary assumptions aside, the cornerstone of both electronic signature and digital signature legislation is the existing common law notion that a signature can take the form of any mark so long as it was intended by the signer to validate a writing.[26] Representative of this common law doctrine is Kansas' act which states that "a digital signature may be accepted as a substitute for, and, if accepted, shall have the same force and effect as, any other form of signature."[27]

III. THE BASICS OF DIGITAL SIGNATURE TECHNOLOGY AND VERIFICATION

There are numerous ways to create digital signatures.[28] These methods range from simple acts, such as typing your name on an e-mail message, to more elaborate and secure acts, such as fingerprint or voice scans.[29] One thing that each of these identification features have in common is that none resembles a traditional handwritten signature. Instead, the "signature" takes the form of letters, numbers, and/or symbols

---

manner, and relied upon reasonably and in good faith) *with* FLA. STAT. ANN. §§ 282.70-75 (West 1998) (failing to establish any evidentiary presumptions concerning the identity of the sender of the message or the integrity of the message's content).

26. Brown v. Butchers and Drovers' Bank, 6 Hill 443, 444 (N.Y. 1844) ("A person may be bound by any mark or designation he thinks proper to adopt, provided it be used as a substitute for his name."). As noted in an early opinion by the Illinois Supreme Court:

> We think it makes no difference, so far as the defendant's liability is concerned whether he wrote his name in script or Roman letters, or whether such letters were made with a pen or with type, or whether he printed, engraved, photographed or lithographed them, so long as he adopted and issued the signature as his own. It is true, that a written signature in script, may be a safer mode of subscribing one's name, but where a party has adopted a signature made in any other mode, and had issued an instrument with such adopted signature, for value, he is estopped from denying its validity.

Weston v. Myers, 33 Ill. 424, 432 (1864).

27. KAN. STAT. ANN. § 60-2616(c) (Supp. 1997). *See also* MINN. STAT. ANN. § 325K.19(4)(b) (West 1998) (stating that a verified electronic signature satisfies the legal requirements of a signature); UTAH CODE ANN. § 46-3-401 (1998) (stating that a verified digital signature satisfies the legal requirements of a signature); FLA. STAT. ANN. § 282.73 (West 1998) (noting that "an electronic signature may be used to sign a writing and shall have the same force and effect as a written signature."). The flexibility of this common law doctrine has enabled courts to expand its meaning to account for all kinds of modern technologies. *See, e.g.,* United States v. Miller, 70 F.3d 1353 (D.C. Cir. 1995) (holding that the unauthorized use of a PIN number to withdraw funds was forgery insofar as it was "tantamount to cashing a check with a forged signature."); Spevak, Cameron & Boyd v. National Comm. Bank of New Jersey, 677 A.2d 1168 (App. Ct. N.J. 1996) (finding that using an account number as an endorsement constituted a signature).

28. Greenwood & Campbell, *supra* note 5, at 309.

29. *Id.* Analogous verification procedures for creating electronic signatures include: "magnetic stripe cards with personal identification numbers (PIN's), user names and passwords, public-key cryptography, writing tablets with electronic pens, and even smart cards that generate a unique access code every few seconds." *Id.*

juxtaposed through a series of mathematical formulas, or algorithms.[30]

Although there are many methods for creating a digital signature, one of the most widely used technologies for authentication purposes today is known as "public key" or "asymmetric cryptography."[31] Asymmetric cryptography is accomplished by implementing encryption/decryption software, a process in which the message and signature can be scrambled by the sender and unscrambled by the recipient using the same type of electronic "key pairs."[32] First, the transmitter, using a "private key" known only to him or her, encrypts the message and signature with a pass-phrase (e.g., personal identification number) and sends it to the recipient.[33] The resulting encryption is the digital signature or "hash result,"[34] which is unique to each document and, thus, produces a new hash result or "signature" with each transmission.[35]

---

30. Closen & Richards, *Lost in Cyberspace, supra* note 4, at 734-35. For example, when printed a digital signature looks something like this:
—Digital Signature—
owHtWX1sU1UUP+91G+22ysbHnDHcBeZAVmq7L9iAuNJ2UuhX2suUSpaufVsftu8£
y1kUXTGsGHAgsE
—End Signature—
ILLINOIS ACT, *supra* note 18, at 18 cmt. 4.

31. Greenwood & Campbell, *supra* note 5, at 310; Closen & Richards, *Lost in Cyberspace, supra* note 4, at 734. *See also* Anthony Martin Singer, Note, *Electronic Commerce: Digital Signatures and the Role of the Kansas Digital Signature Act*, 37 WASHBURN L. J. 725, 729 (1998) ("The technology most associated with digital signatures is asymmetric encryption.").

32. DIGITAL SIGNATURE GUIDELINES, *supra* note 16, at 8; Michael D. Wims, *Law and the Electronic Highway: Are Computer Signatures Legal?*, CRIMINAL JUSTICE MAG., Spring 1995, at 31.

33. Closen & Richards, *Lost in Cyberspace, supra* note 4, at 735.

34. Kenneth A. Freeling & Ronald E. Wiggins, *States Develop Rules for Using Digital Signatures: Laws That Govern Transactions Using Public Key Cryptography Will Spur Electronic Commerce*, NAT'L L. J., Oct. 20, 1997, at C11; DIGITAL SIGNATURE GUIDELINES, *supra* note 16, at 9.

35. Closen & Richards, *Lost in Cyberspace, supra* note 4, at 736. This unique two-key system is central to the security of public key encryption technology. By comparison, consider the most commonly used verification process known as "private key" or "symmetric" electronic cryptography. *See generally* Dorney, *supra* note 19, at 145; Phillip E. Reiman, *Cryptography and the First Amendment: The Right to be Unheard*, 14 J. MARSHALL J. COMPUTER & INFO. L. 325, 328 (1996); Wyrough & Klien, *supra* note 5, at 422. In symmetric cryptography, text is created and deciphered using a single key. Dorney, *supra* note 19, at 145. Thus the same secret key is used by both the sender to encrypt data and by the recipient to decrypt it to its original form. *See* Charles R. Merrill, *Proof of Who, What and When In Electronic Commerce Under the Digital Signature Guidelines*, 525 PLI/Pat 129, 133 (1998); Dorney, *supra* note 19, at 145; *see* Reiman, at 329; Wyrough & Klein, *supra*, note 5 at 422. Therein lies the principle weakness of symmetric cryptography. For example, if, during the exchange of information, an unauthorized third party intercepts the key, then he or she can pose as the authorized sender of the transmission. *See* Dorney, *supra* note 19, at 145; Wyrough & Klein, *supra note 5*, at 422; Greenwood & Campbell, *supra* note 5, at 310-11. Moreover, because the key is not unique to each user, its use permits repudiation

After receiving the document, the recipient runs a program and decrypts the sender's document and signature by using the "public key" (which is made publicly available online) to the encrypting private key.[36] The program then compares the private key with the public key to determine if the document sent has been altered since its original transmission.[37] If unaltered, the two keys will match and the recipient can be reasonably confident that the subscriber actually executed the document.[38] If, however, the document was changed between execution and verification the hashes will differ, meaning that the signature has in some way been compromised and will fail verification.[39]

The security of asymmetric cryptography may be enhanced by adding length to the key pairs.[40] By increasing the possible key pairs to be deciphered, the likelihood that a "hacker" can randomly decode the numerous combinations is significantly reduced. Even with a strong algorithm, a public key pair with a short key length can be "cracked" by the "brute force" approach using the random generation of all of the possible public/private key pair combinations for a given public key until the third party uncovers the correct private key.[41] While longer key pairs provide heightened security in asymmetric cryptography, even professional cryptographers point out that no encryption scheme is completely invulnerable.[42] Nevertheless, digital signature technology which imple-

---

by the sender of the message (i.e. it is possible for the sender to claim that someone else compromised the key and avoid liability). *See* Dorney, *supra* note 19, at 145. Because of these deficiencies, most security-conscious states to have enacted comprehensive digital signature legislation have adopted the asymmetric methodology, which eliminates the need for users to share a secret key and, thus, reduces the risks associated with single key cryptography. *See* Dorney, *supra* note 19, at 145; Greenwood & Campbell, *supra* note 5, at 313; Lonnie Eldridge, *Internet Commerce and the Meltdown of Certification Authorities: Is the Washington State Solution a Good Model?*, 45 UCLA L. REV. 1805, 1811 (1998). *See, e.g.*, UTAH CODE ANN. § 46-3-103(2) (1998).

36. Merrill, *supra* note 35, at 131; Robertson, *supra* note 5, at 820.

37. Closen & Richards, *Lost in Cyberspace, supra* note 4, at 736.

38. John B. Kennedy & Shoshana R. Davids, *Bartleby the Cryptographer: Legal Profession Prepares for Digital Signatures*, N.Y. L.J., Jan. 22, 1996, at S4.

39. *Id;* Greenwood & Campbell, *supra* note 4, at 314; DIGITAL SIGNATURE GUIDELINES, *supra* note 16, at 35 cmt. 1.11.2.

40. *See* Dorney, *supra* note 19, at 146 (stating that the greater the length of key, the more difficult it is to corrupt); Christy Tinnes, Student Work, *Digital Signatures Come to South Carolina: The Proposed Digital Signature Act of 1997*, 48 S.C. L. REV. 427, 429 (1997) (stating that while the industry standard is a 40-bit key, longer keys provide better security).

41. Dorney, *supra* note 19, at 145-46.

42. *Id*; *see also* Victoria Slind-Flor, *Moving Into Cyberspace as Notaries, The Need to Authenticate Electronic Documents Is a New Frontier for Attorneys*, 18 NAT'L L. J. 16 (1995) (stating that the encryption system is vulnerable to corruption); Elizabeth Wasserman, *Signing on with Digital Signatures—New Laws May Allow Computer Validation*, PHOENIX GAZ., Aug. 29, 1995, at A1 (noting that no computer system is perfectly secure). *See gener-*

ments cryptographic methodology is still considered very secure in that, while not absolutely fool-proof, it is "computationally impossible" to deduce one key solely from knowledge of the other key.[43]

IV. CERTIFICATION AUTHORITIES ("CYBERNOTARIES")

An integral part of the digital signature verification process is determining whether the person who sent the message is really who he or she purports to be. This authentication function is rooted deep in history, having been performed for the past 350 years by public officers known as notaries public.[44] Similarly, current cryptographic protocols dictate that cyber-verifications are to be accomplished by neutral and trusted third parties called certification authorities or "cybernotaries"[45] (hereinafter certification authorities). As the term implies, there are inherent similarities between traditional notaries public and certification authori-

---

ally Gary W. Fresen, *What Lawyers Should Known About Digital Signatures*, 170 ILL. B. J. 85 (1997).

43. BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C § 2.6, 33-40 (2d ed. 1996). *See also* Greenwood & Campbell, *supra* note 4, at 314 (stating that "public-key cryptography allows people and businesses to exchange messages over open networks with a high degree of confidence that those messages are confidential . . ., authentic . . ., and accurate . . ."); Wright, *supra* note 7, at 194 ("Public-key cryptography can be very effective in showing whether a particular document was signed with a certain private key."); Biddle, *supra* note 11, at 1144 (noting that "a well-functioning public key infrastructure could allow private individuals, businesses, and government to routinely and securely conduct . . . [business] . . . over . . . the Internet"); Eldridge, *supra* note 35, at 1807-08 ("Public-key cryptography allows parties . . . to exchange information safely . . .");

44. *See* Michael L. Closen, *The Public Official Role of the Notary*, 31 J. MARSHALL L. REV. 651, 701 (1998) (noting that "[n]otaries have been on the North American continent for more that 350 years."). Notaries are, by and large, considered public officials. *See, e.g.*, Closen, *supra*, at 651 (stating that a notary is a public official); RICHARD B. HUMPHREY, THE AMERICAN NOTARY MANUAL 209 (4th ed. 1948) (stating that "[t]he office of notary pubic is a public office . . ."); Britton v. Niccolls, 104 U.S. 757, 765 (1881) (stating that a notary is a public official); May v. Jones, 14 S.E. 552, 553 (Ga. 1891) (stating "the notary . . . is a public officer, sworn to discharge his duties properly"). *But see* Transamerica Ins. Co. v. Valley Nat'l Bank, 462 P.2d 814, 817 (Ariz. App. 1969) ("designat[ing] a notary public as . . . , at best, . . . quasi-public [in] nature"); OR. REV. STAT. § 194.010(6) (1996) (indicating that notarial acts are not considered official duties under the Oregon Constitution).

45. Closen & Richards, *Lost in Cyberspace, supra* note 4, at 737; Merrill, *supra* note 35, at 134; Robertson, *supra* note 5, at 820; Brian W. Smith, *Digital Signatures: The State of the Art of the Law*, 114 BANKING L.J. 506, 508 (1997); A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 49 (1996). *See also* Michael L. Closen & G. Grant Dixon III, *Notaries Public From the Time of the Roman Empire to the United States Today, and Tomorrow*, 68 N.D. L. REV. 873, 875 (1992) (describing notaries as highly trustworthy). The phrase "cybernotary" was coined by the American Bar Association to describe persons engaged in the certification and authentification functions surrounding online transactions. John C. Yates, *Recent Legal Issues in Electronic Commerce and Electronic Interchange*, 430 PRAC. L. INST. 271, 300 (1996).

ties.[46] Both are creatures of statute.[47] Both are typically licensed or commissioned by the state.[48] Both engage primarily in the process of identification.[49] Both occupy a position of public trust.[50] And certification authorities will, as notaries now do, eventually affect commercial transactions worth thousands or millions of dollars annually.[51]

Despite these general similarities, the functional differences between certification authorities and notaries public are many and varied. For instance, unlike their contemporary counterparts, certification authorities may, but need not be, human beings. Certification authorities can, for example, take the form of financial institutions, accounting firms, trust companies, and the like.[52] Moreover, while current notarial law requires the signer of the document to personally appear before the notary in order to confirm the person's identity,[53] cybernotarial legislation dictates that a certification authority's acknowledgment of a digital signature is valid whether the signer physically appeared before the certification authority when the digital signature was created so long as certain procedural requirements are followed.[54]

Perhaps the most significant difference between certification authorities and traditional notaries public is that certification authorities use sophisticated computer technology with which to identify document signers. As a result, certification authorities need a good working knowledge of computer technology to function efficiently and effectively.[55] By com-

46. *See* DIGITAL SIGNATURE GUIDELINES, *supra* note 16, at 31 cmt. 1.6.3 (stating that cybernotaries' role is to mimic those of the common law notary, and typically practice in international, computer-based transactions).

47. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 739 ("Cybernotaries . . . are regulated by statute."); RICHARD B. HUMPHREY, THE AMERICAN NOTARY MANUAL 209 (4th ed. 1948) (stating "the law is sole source of [the notary's] authority . . .).

48. Closen & Richards, *Lost in Cyberspace, supra* note 4, at 739. Unlike notaries public, who must be licensed by the state to act, licensing of cybernotaries is voluntary in most states. *See, e.g.*, WASH. REV. CODE ANN. § 19.34.100(7) (West 1998).

49. *See* Biddle, *supra* note 11, at 1178-79.

50. *See* Gombech v. Department of State, 692 A.2d 1127, 1132 (Pa. Commw. Ct. 1997) (referring to the office of notary as a "position of public trust."); Farm Bureau Fin. Co. v. Carney, 605 P.2d 509, 514 (Idaho 1980) (finding that "the notary [is] a public officer in a position of public trust"); Closen & Richards, *Lost in Cyberspace, supra* note 4, at 757 (stating that "cybernotaries . . . will occupy positions of esteem.").

51. Closen & Richards, *Supernotaries, supra* note 10, at A19.

52. Froomkin, *supra* note 45, at 55. *See also* Dorney, *supra* note 19, at 148 (describing certification authorities as "organizations"); Wyrough & Klien, *supra* note 5, at 426 ("Certification [a]uthorities can be either public or private entities"); MINN. STAT. ANN. § 325K.01 (Subd. 5) (West 1998) ("'Certification' authority means a person who issues a certificate").

53. *See* R. Jason Richards, *Stop! . . . Go Directly To Jail, Do Not Pass Go, and Do Not Ask for a Notary*, 31 J. MARSHALL L. REV. 879, 880 (1998).

54. UTAH CODE ANN. § 46-3-405 (Supp. 1998).

55. *See* Glen-Peter Ahlers Sr., *The Impact of Technology on the Notary Process*, 31 J. MARSHALL L. REV. 911, 925 (1998) ("While much of the digital signature technology can be

parison, consider that the most sophisticated technology associated with the notary profession is the notary seal. The notary seal, which evolved slowly over time, progressing from the waxen seal of early Rome to the present day inked stamp or metal embosser,[56] is sometimes used incorrectly,[57] and is even being eliminated as a requirement on paper documents in some states.[58] Suffice it to say that certification authorities will be quite different from yesterday's notary in both practice and expertise.[59] Therefore, while the computer knowledge required of certification authorities will not per se bar traditional notaries from becoming certification authorities in most states, many commentators believe it is unlikely many of today's notaries will qualify for or have the supporting computer systems necessary to fulfill the certification authority role. No doubt this will lead to a concentration of digital signature notarial services in the hands of a few highly qualified certification authorities.[60] To ensure the necessary level of sophisticated personnel, many commentators believe and some state statutes have mandated, that certification

automated and does not require an engineering degree to operate, a basic understanding of how computers transfer data among other computers is required."); Slind-Flor, *supra* note 42, at 16 (noting that cybernotaries will "requir[e] a good understanding of technology in general . . .") (quoting Richard L. Field, a sole practitioner, and a member of the American Bar Association committee on cybernotaries).

56. *See* Karla J. Elliot, *The Notary Seal—The Last Vestige of Notaries Past*, 31 J. MARSHALL L. REV. 903, 907 (1998); *see also* NOTARY LAW, *supra* note 4, at 11 ("Seals have been used to denote a document's authenticity since the days of the Roman Empire when an officer called a *Notarius* might impress a seal of metal, mineral or bone, often worn as a ring, into hot wax.")

57. Unfortunately, even the minimal tasks associated with affixing a notary seal all too often results in negligent notarial conduct, thus calling into question some notaries' ability to become cybernotaries. *See* Closen & Richards, *Lost in Cyberspace*, *supra* note 4, at 715 (stating that many of "today's notaries are incapable of performing the most basic functions of the office (such as . . . affixing notary seals . . .")).

58. Interestingly, about a dozen states have abolished the obligation of notaries public to use a notary seal. *See* Vincent Gnoffo, Comment, *Notary Law and Practice for the 21st Century: Suggested Modifications for the Model Notary Act*, 30 J. MARSHALL L. REV. 1063, 1064-65 (discussing the abolishment of the notary seal requirement). For excellent discussions of the history of the notary seal, see generally Elliot, *supra* note 56; Eric Mills Holmes, *Stature and Status of a Promise Under Seal as a Legal Formality*, 29 WILLAMETTE L. REV. 617 (1993).

59. *See* NOTARY LAW, *supra* note 4, at 500.

60. NOTARY LAW, *supra* note 4, at 500. *See also* WARWICK FORD & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE: BUILDING THE INFRASTRUCTURE FOR DIGITAL SIGNATURES AND ENCRYPTION 375 (1997) (stating that "many notaries who perform traditional identity confirmation functions essential to secure electronic commerce are not stereotypical technology-based trusted third parties (such as Certification Authorities), in that they do not perform the technology-based functions [required], or may not make digital communications a part of their notarial activities"). *Cf.* Ahlers, *supra* note 55, at 912 ("Instead of causing the death of notaries public, technologies might instead increase their importance.").

authority eligibility be limited to a select few individuals or professional organizations (e.g., attorneys, financial institutions, title insurance companies, and government agencies).[61]

Regardless of what or who fulfills the role of certification authority, a certification authority's principle function remains. That function is to bind the sender's private key with the recipient's public key, similar to the way that a notary public would sign and perhaps affix a seal to validate the original execution of a handwritten signature.[62] If the verification is successful, the certification authority digitally signs and issues a "certificate,"[63] which is a computer generated record that identifies the subscriber as well as the public key and represents that the signer identified in the certificate holds the corresponding private key.[64] This certificate is then placed in an electronic storage facility called a public repository.[65] Then, a recipient of a digitally signed message will access the certificate and determine that a public key is associated with a private key possessed by a particular person, obtain a copy of that public key, and then use that public key to decrypt the digitally-signed message

---

61. *See, e.g.,* DIGITAL SIGNATURE GUIDELINES, *supra* note 16, at 31 cmt. 1.6.3. (recommending cybernotaries be "attorneys at law admitted to practice in the United States and qualified to act as a CyberNotary pursuant to specialization rules currently under development"); Slind-Flor, *supra* note 42, at 16 (positing that cybernotaries will inhabit "a high-level legal position . . . requiring a good understanding of contract law, international law, technology in general, and [such lawyers will] very likely need to have a substantial legal infrastructure around them"). *See also* Shinichi Tsuchiya, *A Comparative Study of the System and Function of the Notary Pubic in Japan and the United States* (May 30-June 1, 1996) *in* Nat'l Notary Ass'n, Jan. 1997 (available from the National Notary Association). "It is necessary to have Notaries or CyberNotaries who have acquainted themselves not only with computer technologies, but also with electronic transactions and related laws. For this reason, CyberNotaries should be lawyers." *Id.*

Unfortunately, though, even limiting the availability of those who may serve as Certification Authorities to "professionals" like attorneys does not ensure that moral or ethical values will prevail in the world of cyberverifications. *See, e.g.,* Iowa State Bar Assoc. v. Baurele, 460 N.W. 2d 452 (Iowa 1990) (imposing indefinite suspension of attorney-notary's license for falsely certifying documents); Iowa State Bar Assoc. v. O'Donohoe, 426 N.W.2d 166, 166 (Iowa 1988) (reprimanding attorney-notary for "knowingly making a false statement on a document filed for public record"). *See generally* Christopher B. Young, *Signed, Sealed, Delivered . . . Disbarred? Notarial Misconduct by Attorneys*, 31 J. MARSHALL L. REV. 1085 (1998).

62. Closen & Richards, *Lost in Cyberspace, supra* note 4, at 740; Tinnes, *supra* note 40, at 429.

63. A "certificate" is a "computer based record which: (a) identifies the Certification Authority issuing it; (b) names or identifies its subscriber; (c) contains the subscriber's public key; and (d) is digitally signed by the Certification Authority issuing it." UTAH CODE ANN. § 46-3-103(3) (1998).

64. Brian W. Smith, *Digital Signatures: The State of the Art of the Law*, 114 BANKING L. J. 506, 508 (1997); Robertson, *supra* note 5, at 820.

65. A "repository" is "a system for storing and retrieving certificates and other information relevant to digital signatures." UTAH CODE ANN. § 46-3-103(29) (1998).

the recipient received.[66]

V. CRITICISM OF UTAH'S DIGITAL SIGNATURE ACT[67]

In 1995, Utah adopted the nation's first comprehensive legislation concerning digital signatures. The Utah Act purports to effectuate the following purposes:

> (1) to facilitate commerce by means of reliable messages;
> (2) to minimize the incidence of forged digital signatures and fraud in electronic commerce;
> (3) to implement legally the general import of relevant standards, such as X.509 of the International Telecommunication Union . . . ; and
> (4) to establish, in accordance with multiple states, uniform rules regarding the authentication and reliability of electronic messages.[68]

Because of the evolving nature of digital signature technology, Utah included within its comprehensive legislative framework a provision establishing the Division of Corporations and Commercial Code. It is the Division's role to make rules and regulations governing Certification Authorities beyond the general guidelines already established in the statute—in short, to adopt the rules needed to implement the act. Perhaps due to the uncertainties surrounding how to develop widespread, yet flexible legislation in electronic commerce, several of the provisions in the Utah Act are vague, confusing, or altogether inadequate to deal with the sophisticated nature of electronic transactions. The effect of this uncertainty is to raise serious concerns as to the Act's overall effectiveness and, moreover, how it is to be interpreted by the consuming public as well as by the Division designated to implement it.

The sections that raise the most concern include the following:

- *Record-keeping.* The division shall specify reasonable requirements for record-keeping by licensed certification authorities.[69]
- *Personnel.* To obtain and keep a license a certification authority shall employ only individuals who are knowledgeable and proficient in following the Act's requirements.[70]
- *Criminal Conviction.* To obtain and keep a license a certification authority shall employ only persons who have not been convicted of a felony or a crime involving fraud, false statement, or deception.[71]

---

66. Robertson, *supra* note 5, at 821.

67. For a more thorough discussion of the regulatory provisions of Utah's digital signature act, see generally Biddle, *supra* note 11, at 1153-63; Eldridge, *supra* note 22, at 1828-35.

68. UTAH CODE ANN. § 46-3-102 (Supp. 1998).

69. *Id.* § 46-3-104.

70. *Id.*

71. *Id.* § 46-3-201.

• *Recommended Reliance Limit.* Certification authorities are authorized to specify a recommended reliance limit (i.e., bond) beyond which the recipient should not rely.[72]

• *Suitable Guaranty.* To obtain and keep a license a certification authority shall file with the division a suitable guaranty.[73]

• *Residency Requirement.* To obtain and keep a license a certification authority shall maintain an office (or designate a registered agent for service of process) in the State.[74]

• *Security System Requirements.* Licensed certification authorities are required to use trustworthy systems.[75]

• *Limited Liability.* Any persons who knowingly or intentionally violate the act are subject to civil penalties up to $5,000 per violation or 90% of the recommended reliance limit of a material certificate, whichever is less.[76]

• *Reasonable Care Requirement.* Subscribers must exercise reasonable care to retain control of their private keys.[77]

• *Legal Presumptions.* In court-adjudicated disputes, it is presumed that a licensed certification authority's digitally signed certificate is authentically issued by a licensed certification authority and accepted by the subscriber, and that the information listed and confirmed in such a certificate is accurate.[78]

A. Record-keeping Requirement

As originally adopted in 1995, the Utah Act did not include a record-keeping requirement.[79] This changed in 1996, when Utah amended its Act to specifically authorize the Division to include reasonable requirements for record-keeping by licensing certification authorities.[80] This requires that certification authorities keep an archive of certificates that are suspended, revoked, or expired.[81] While Utah should be applauded for amending its statute to include a record-keeping requirement, its provision falls both short and wide of the mark. At least three problems arise from this record-keeping requirement.

First, the provision is underinclusive in that it obligates the certification authority to keep records of only a limited number of certificates,

72. *Id.* § 46-3-309.
73. Utah Code Ann. § 46-3-309.
74. *Id.*
75. *Id.* § 46-3-301.
76. *Id.* § 46-3-203 (Supp. 1998).
77. *Id.* § 46-3-305.
78. Utah Code Ann. § 46-3-406.
79. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 748.
80. Utah Code Ann. § 46-3-104(e) (Supp. 1998).
81. *Id.* § 46-3-501(2)(f).

which, by implication, have been compromised in some way. By definition, then, all other electronic communications between the certification authority and subscribers may be destroyed. This is an inappropriate standard for at least two reasons. First, in practice this standard would permit the obliteration of the vast majority of certificates, because most transactions should proceed without complications. Such an approach is inadequate because it fails to meet the needs and expectations of consumers. Undoubtedly there will be requests from subscribers for duplicate certificates even though the digital signature transaction was executed flawlessly.[82] Second, the Utah Act provides that in executing a certificate, a certification authority must comply with all material requirements of the Act.[83] Thus it is reasonable for the document signer to expect that the authentication is being performed correctly and that any challenge to its validity will fail.[84] To that end, the document signer has a right to expect that, if called upon, the certification authority could produce documentation that the signature on the instrument was authenticated in accordance with statutory requirements.[85] This proposal is no more burdensome than the present system of record-keeping expected in our own personal and business affairs.[86] Furthermore, notaries public, whose identification functions closely resemble those of certification authorities', are in many states required to keep journals of their official acts[87] and make such records available to the public upon reasonable

82. "Records that are typically required to be maintained and made available upon authorized request include documentation of a Certification Authority's compliance with the applicable CPS [Certification Practice Statement] and documentation of actions and information material to each certificate application and to each certificate issued." FORD & BAUM, *supra* note 60, at 375.

83. Utah Code Ann. § 46-3-309(2)(A) (Supp. 1998) .

84. *See* Peter J. Van Alstyne, *The Notary's Duty to Meticulously Maintain a Notary Journal*, 31 J. MARSHALL L. REV. 777, 779 (1998).

85. *See* Van Alstyne, *supra* note 84, at 779.

86. See Van Alstyne, *supra* note 84, at 779 (citing *Safety Spelled J-O-U-R-N-A-L*, NAT'L NOTARY MAG., Nov. 1996, at 16-18). As Mr. Van Alstyne points out:

> [t]he keeping of certain records is an inherent responsibility of nearly every responsible adult. For example, record keeping is vital to the survival and legal protection of any business enterprise. As taxpayers, we must be prepared to produce personal financial records in the event of a tax audit. In many ways, the failure to maintain a minimal set of records is negligent behavior.

87. Maintaining a notary journal offers benefits beyond mere statutory compliance. *See generally* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 753 n.314. "The authors have not found a reported appellate case in which a notary who kept a journal entry was sued for negligence in identifying the document signer. But, there have been numerous successful tort suits against notaries (and/or their employers or sureties) who did not keep journal entries and who failed to detect the false identities of signers." *Id.* (citations omitted).

request.[88] The importance of record-keeping in the electronic signature verification process has been widely encouraged. As noted by two leading authorities in electronic commerce:

> Documentation of activities is indispensable to the operation of a trustworthy [c]ertification [a]uthority. The [c]ertification [a]uthority must be able to evidence its proper operations prospectively, as well as after the fact, to support the non-repudiation of transactions undertaken with the certificates it issues . . . . Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate and complete.[89]

Thus, certification authorities should be required to keep a record not only of all "compromised" certificates, but of every certificate issued or rejected.

A second problem with the Utah Act's limited record-keeping requirement is that it fails to adequately ensure that the record of certificates will be protected from the unscrupulous conduct of others.[90] This is because certificates are available via on-line repositories where availability is no longer strictly controlled, meaning that certificates are more vulnerable to unauthorized access and, thus, potential fraud.[91] Therefore, because a large certification authority's database might contain thousands, if not millions, of certificates, it is essential that certification authorities retain written documentation of the certificates issued.[92] The failure to keep adequate documentation may complicate or delay the process by which a "compromised" certificate is suspended or revoked, thus subjecting the certification authority to potential liability to those third parties who reasonably rely on the certificate's validity only to discover later that the certificate is unreliable.[93]

The proper maintenance of a journal can further protect the certification authority from false accusations that a cybernotarial act was per-

---

88. *See* Van Alstyne, *supra* note 84, at 784. Notaries are required to maintain journals or logs in Alabama, Arizona, California, Colorado, Hawaii, Maryland, Mississippi, Missouri, Nevada, Oklahoma, Oregon, Pennsylvania, Tennessee, Texas and the District of Columbia. *Id.* at 778 n.5.

89. FORD & BAUM, *supra* note 60, at 375.

90. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 748.

91. *See* Eldridge, *supra* note 35, at 1824 ("Employers of a CA [Certification Authority] who have access to the certificate database have the potential to cause great harm."); Wyrough & Klein, *supra* note 5, at 415 ("The chances of fraud and unauthorized access increases as more people use networked computers.").

92. "[I]t is essential for . . . databases or repositories to have thorough backup procedures in place. . . . [T]he careless alteration or loss of a certification could have grave consequences." Eldridge, *supra* note 35, at 1820; FORD & BUAM, *supra* note 60, at 375 ("Documentation of activities is indispensable to the operation of a trustworthy CA [Certification Authority].").

93. *See* Dorney, *supra* note 19, at 153.

formed when, in fact, it was not.[94] This prospect presents itself courtesy of the Federal Rules of Evidence, which permits journals to be admitted into evidence under the business records exception to the hearsay rule. Journals may be admitted as evidence if they are kept in the regular course of the business activity and are entered "at or near" the time of the recorded act.[95] Under the Rules of Evidence, if normal circumstances would have dictated that an event be recorded had it taken place, then the nonexistence of a record of the event in a journal can prove the event never occurred.[96] "As most perpetrators will not realize that a journal entry must accompany every [business] act, the absence thereof will be the smoking gun pointing to the perpetrator's misdeed."[97] Thus, keeping a journal record could guard against private individuals with access to the certificate database—so called "insiders"—from using their position to exploit the system.[98] To be sure, just as fraudulent conduct represents one of the greatest concerns in the notary's world of paper transactions,[99] so too will it represent a serious problem in cyberspace.[100] Given that reducing the likelihood of fraud is one of the primary goals in electronic commerce,[101] the need for certification

94. *See* Van Alstyne, *supra* note 84, at 781.

95. FED. R. EVID. § 803(6); Van Alstyne, *supra* note 84, at 780.

96. FED. R. EVID. § 803(7).

97. Van Alstyne, *supra* note 84, at 781-82.

98. *See* Eldridge, *supra* note 35, at 1824.

99. It is not unusual for notaries to have to defend conduct—whether real or imagined—which is brought on by "insiders," who request or direct them to take shortcuts or even use the notary's official seal and "notarize" a document without the notary's knowledge. *See* Van Alstyne, *supra* note 84, at 781; Young, *supra* note 61, at 1102; *see also* Michael J. Osty, *Notary Bonds and Insurance: Increasing the Protection for Consumers and Notaries*, 31 J. MARSHALL L. REV. 839, 853 (1998) ("Despite the fact that one notarizes in a seemingly secure environment, [a] notary can face the danger of an improper notarization and suffer dire financial consequences."). *See, e.g.*, Independence Leasing Corp. v. Acquino, 506 N.Y.S.2d 1003 (Erie County Ct. 1986) (Employer encouraged notary-employee to take shortcuts in performing duties); State Life Ins. Co. v. Faucett, 163 S.W.2d 592 (Mo. 1942) (finding that notary signed a false certificate of acknowledgment, and did nothing to conceal her fraud).

Unfortunately, attorneys who are notaries are guilty of most of these same offenses. *See, e.g.*, Iowa State Bar Assoc. v. Baurele, 460 N.W.2d 452 (Iowa 1990) (imposing indefinite suspension of attorney-notary's license for falsely certifying documents); Iowa State Bar Assoc. v. O'Donohoe, 426 N.W.2d 166, 166 (Iowa 1988) (reprimanding attorney-notary for "knowingly making a false statement on a document filed for public record").

100. *See* Wright, *supra* note 7, at 191 ("Just as risks plague the authentication of paper documents, so too will they plague the authentication of electronic documents."); Closen & Richards, *Lost in Cyberspace*, *supra* note 4, at 732 (noting that "no on-line computer generated transaction seems immune from [fraudulent conduct]"); Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J. L. & TECH. 465, 472 (1997) (noting that computer crime is on the rise).

101. Several states assert as their electronic or digital signature legislation's purpose to, among other things, "minimize the incidence of forged digital [or electronic] signatures and

authorities to maintain a journal cannot be overemphasized.[102]

The third problem with the Utah Act's record-keeping requirement is that certification authorities need only keep an archive of certificates within at least the past three years.[103] By limiting the use of digital signatures to such a short time period, this provision raises serious policy issues. It is ill-advised to limit the availability of documentary evidence for electronic transactions (e.g., contracts, leases, etc.) that may be challenged long into the future.[104] As one commentator cogently stated: "[a]s it would be bad public policy to arbitrarily affix a statute of limitations to the [cybernotarial] act and the [certification authority's] liability for negligently performing it, it is likewise imprudent to arbitrarily affix a term of years over which a [record] should be retained."[105]

> The retention of certification activity records for a designated period of time is indispensable for many [other] reasons [as well], including:
>
> • Support or non-repudiation of digitally signed messages;
>
> • Evidence of a [c]ertification [a]uthority's proper performance to rebut claims of malfeasance; and
>
> • Satisfaction of legislation and regulatory requirements, where applicable.[106]

Thus, just as sound business policy and public policy dictate that certification authorities retain a record of all the certificates that they issue and refuse to issue,[107] it is also essential for certification authori-

---

fraud in electronic commerce." *See, e.g.*, UTAH CODE ANN. § 46-3-102 (1998); FLA. STAT. ANN. § 272.71(3) (West 1998); MINN. STAT. ANN. § 325K.02(2) (West 1998).

102. The importance of maintaining a journal in the notarial profession has been summarized as follows:

> It is every notary's inherent duty of reasonable care to make a careful and complete record of every notarization performed. If properly maintained, the notary's journal will demonstrate that reasonable care was exercised in every aspect of the notarial act. It will further establish that the notary routinely exercises reasonable care in the performance of his or her notarial duties. The notary journal guides the notary through correct notarial procedures for every act, thus minimizing any potential for serious mistakes. As a result, the notary journal is a valuable protection for the notary against groundless accusations of wrongdoing. It is especially useful for refreshing the notary's memory about the notarial act that took place years ago.

Van Alstyne, *supra* note 84, at 778-79; Closen & Richards, *Lost in Cyberspace, supra* note 4, at 752-53.

103. UTAH CODE ANN. § 46-3-501(2)(f) (Supp. 1998).

104. Eldridge, *supra* note 35, at 1831; *see also* DIGITAL SIGNATURE GUIDELINES, *supra* note 16, at 3.5 cmt. 3.5.3.

105. Van Alstyne, *supra* note 84, at 792.

106. FORD & BAUM, *supra* note 60, at 376.

107. *See* Closen & Richards, *Supernotaries, supra* note 10, at A19; Closen & Richards, *Lost in Cyberspace, supra* note 4, at 753; Van Alstyne, *supra* note 84, at 800. *See also* FORD & BAUM, *supra* note 60, at 208 (noting that the generation of a certificate should include "record[ing] appropriate details of the certificate generation process in an audit journal").

ties to carefully preserve and safeguard expired certificates for as long as the terms of the document it appears on remains in force, and, ideally, for many years thereafter.[108]

B. Licensing Requirements

In addition to the problems inherent in the Utah Act's record-keeping requirement noted above, concerns also exist as to the licensing requirement for certification authorities. The Utah Act states that employers must "employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of [the Act]."[109] This provision implicitly requires that employers of certification authorities hire individuals with a good working knowledge of computer technology in general and digital signature technology in particular. Admittedly, this is a worthwhile goal. But, who determines whether certification authority employees meet these qualifications? At present, employers do. Permitting employers to police themselves as to the qualifications of their own employees to serve as certification authorities is tantamount to putting the "fox in the chicken coop." The only independent evaluation of a certification authority's qualifications are annual performance audits by licensed authorities. Unfortunately, however, these audits have the practical effect of "shutting the stable door after the horse has been stolen."[110] Indeed, a full year could pass before a beginning certification authority is investigated, if at all. To be sure, a significant amount of damage could be done by negligent, illiterate, or even illegally motivated certification authorities before that time.[111] Such omissions should concern both prospective certification authorities

---

108. *See* Van Alstyne, *supra* note 84, at 792 ("The notary should be required to retain the journal for life.") *Cf.* Ford & Baum, *supra* note 60, at 376 (recommending that Certification Authorities retain records for "no more than 30 years after the date a certificate is revoked or expired"). *See also* Digital Signature Guidelines, *supra* note 16, at 3.5 cmt. 3.5.3. The ABA's comment section states:

> The record retention period may depend upon various factors, including: contractual obligations to subscribers, statutory record retention requirements, and business needs. For example, digital signatures used in land transactions may be contestable for a period specified under local land registry laws, and must be accessible during such period. Subscribers to a Certification Authority involved in land transactions would therefore have a business need for record retention over that period.

Id.

109. Utah Code Ann. § 46-3-201(1)(b).

110. *See* John Bartlett, Familiar Quotations 141 n.10 (16th ed. 1992) ("When the horse has been stolen, the fool shuts the stable." (quoting Les Proverbes del Vilain, MS Bodleian (c. 1303)).

111. "Using a Certification Authority's services can involve a considerable amount of risk and complication even when all parties are acting in good faith. When active subversion of the system is attempted, the risk can be even greater." Eldridge, *supra* note 34, at 1823.

as well as those who will look to certification authorities to provide competent and professional service.[112]

The statute fails to establish even minimal standards to insure that certification authorities fully understand the responsibilities of their office prior to becoming licensed certification authorities. For instance, there are no age requirements, no specific experience requirements and no education requirements. In short, certification authorities are not required to exhibit in any way a floor level of competency (other than to their own employers, as noted above) of the digital signature verification process before becoming licensed, practicing certification authorities. Indeed, "[a]n elementary school dropout could become a [certification authority] and affect commercial transactions worth millions of dollars."[113]

It makes little sense to subject certification authorities to civil penalties and the possible suspension or revocation of their licenses for misfeasance, and at the same time fail to require any instruction, testing or training on how to adequately perform their jobs.[114] Surely it would be prudent to insist, at a minimum, that certification authorities reach the age of majority and undergo a course of study in the technology, law, and ethics of electronic commerce before unleashing them into the electronic marketplace.[115]

Perhaps aware of the potential pitfalls in Utah's qualification requirements, some state laws either suggest or mandate higher qualification standards for certification authorities. For example, in addressing the issue of competency newly licensed certification authorities, Mississippi's Digital Signature Act states: "(2) The Secretary of State shall license private [c]ertification [a]uthorities, *conditioned* upon their showing: (a) That they possess proficiency in encryption technology[.]"[116] Similarly, Washington addresses the matter of re-testing certification authorities in its Electronic Authentication Act, where it requires that the Secretary "provide, by rule, for a system of license renewal, which may include requirements for continuing education."[117]

These Acts represent an improvement over the Utah statute for the simple reason that they at least consider some of the significant concerns addressed by commentators.[118] Still, however, even the promising provisions such as those noted above typically take the form of suggestions rather than mandatory requirements. Merely "suggesting" that certification authorities meet the most minimal standards required of the office

112. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 746.
113. *See* Closen & Richards, *Supernotaries, supra* note 10, at A19.
114. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 755.
115. *See* Closen & Richards, *Supernotaries, supra* note 10, at A19.
116. MISS. CODE ANN. § 25-63-7 (1998) (emphasis added).
117. WASH. REV. CODE ANN. § 19.34.101 (West 1998).
118. *See generally* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 755-56.

of certification authority is insufficient to ensure compliance; more direct legislative action is needed. The office of certification authority is simply too important to leave basic requirements such as the education and testing of certification authorities to chance. Unfortunately, though, even these rudimentary requirements are rarely considered by legislators. Indeed, the vast majority of state certification authority laws do not address such issues as age requirements, education, legal and ethical awareness, statutory requirements, and legal liability at all. Much more significant state action is required to ensure that certification authorities meet the needs and expectations of those parties who will expect competent and knowledgeable certification authorities to authenticate their digital signatures.

C. Criminal Convictions

The Utah Act's statute bans anyone who has been convicted of a felony or a crime involving fraud, false statement, or deception from operating as a certification authority.[119] This requirement helps keep potentially unscrupulous persons from serving as licensed certification authorities. This provision is troublesome in that it is both underinclusive and overinclusive. The requirement is underinclusive in that it creates a statutory loophole by failing to disqualify those persons who may have a record of fraudulent conduct in a civil or administrative proceeding.[120] The provision is overinclusive in that while it is entirely reasonable to exclude those applicants who committed fraudulent acts from becoming certification authorities, the same thing cannot be said for prohibiting *all* those individuals who have committed felonies, from being licensed certification authorities. In some cases, the punishment (i.e. exclusion from serving as a certification authority) may not fit the crime.

For instance, what about a non-violent offense such as a felony conviction for involuntary manslaughter? Does such a crime warrant absolute exclusion from becoming a certification authority? It is fair to say that such crimes have little, if anything, to do with honesty or integrity of the kind Utah's Digital Signature Act is designed to prevent. It is fair to say, then, that in totally banning persons convicted of a felony from becoming licensed as certification authorities, Utah's law does too much.[121] Of course, this does not mean that true "criminals" should be

119. Utah Code Ann. § 46-3-201(1)(b) (1998).

120. *See* Closen & Richards, *Supernotaries, supra* note 10, at A19.

121. *See* Richards, *supra* note 53, at 889. It should be noted that the absolute ban against convicted persons has not been followed by every state that has enacted cybernotarial legislation. In Washington, for example, the prohibition extends only to persons who have "been convicted within the past fifteen years of a felony or have ever been convicted of a crime involving fraud, false statement, or deception." Wash. Rev. Stat. Ann. § 19.34.100(1)(b) (West 1998). Nevertheless, Washington's Act is still unacceptable in that

allowed to serve as certification authorities. Quite the contrary—all previous felony convictions should be thoroughly investigated to determine the eligibility status of certification authority applicants. But, upon discovery of a felony conviction, a more equitable and rational means of accessing the qualifications of certification authorities would be to "give those persons convicted of [such] offenses the opportunity to explain away their crime—to defend prior misconduct that may or may not call into question their ability to hold [cybernotarial] office."[122] This sound equitable directive should be fully acceptable to both those seeking to become, and those seeking to ensure the highest standards of, certification authorities. certification authority applicants should be thoroughly investigated in order to determine their individual qualifications to hold cybernotarial office. Remarkably, even if a potential certification authority's application reveals that he or she has a prior criminal conviction, the Utah Act fails to provide that anyone investigate the alleged misconduct contained therein.[123] The failure to provide for an investigative arm of the government to review applications in such a high-tech and fraudulent-prone industry is not indicative of a progression into the new millenium, but rather is reminiscent of replicating the failed policies of the past. Again, it is appropriate to draw an analogy from the tarnished image of the notary pubic, where "it is not uncommon for notary applicants to lie on their applications concerning past offenses," and where illegal conduct is a routine occurrence.[124] It has been said that insanity is, by definition, doing the same thing and expecting different results.[125]

---

it retains a fifteen-year period within which the disgrace of a conviction remains. Any such stigma should be removed from Certification Authority legislation altogether. *See also* MINN. STAT. ANN. § 325K.05(2) (West 1998). To obtain or retain a license, a Certification Authority must employ as operative personnel only persons who have not been convicted within the past 15 years of a felony or a crime involving fraud, false statement, or deception.

122. Richards, *supra* note 53, at 890.

123. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 746.

124. Richards, *supra* note 53, at 888 n56. *See, e.g., Police Say Man Lied About Criminal Past,* ALLENTOWN MORNING CALL, Apr. 9, 1997, at B3. Unfortunately, the occurrence of illegal conduct in notarial practice dates back to this country's first appointed notary. "The American Colonies' first Notary was Thomas Fugill. Appointed in 1639 in the New Haven Colony, he miserably failed to live up to his duties and was thrown out of office for falsifying documents." *Notaries Public in American History,* NOTARY BULL., Apr. 1997, at 3. *See also* Florida Bar v. Farinas, 608 So.2d 22 (Fla. 1992) (holding illegal conduct of attorney-notary in failing to personally acknowledge signature before notarizing document warranted public reprimand); Iowa State Bar. Assoc. v. Bauerle, 460 N.W.2d 452 (Iowa 1990) (imposing indefinite suspension of attorney-notary's license for falsely certifying documents); Iowa State Bar. Assoc. v. O'Donohoe, 426 N.W.2d 166, 166 (Iowa 1988) (reprimanding attorney-notary for "knowingly making a false statement of fact on a document filed for pubic record"); State Life Ins. v. Faucett, 163 S.W.2d 592 (Mo. 1942) (finding that notary signed a false certificate of acknowledgment, and did nothing to conceal her fraud).

125. Interview with Craig Anderson (Nov. 26, 1998).

This point is particularly applicable here, where "[i]t would be just plain silly to allow the obvious problems of notaries public to continue to plague the office of . . . [c]ertification [a]uthorities into the future."[126]

D. Recommended Reliance Limit

In an effort to assure a level of financial responsibility for certification authorities, the Utah Act creates a recommended reliance limit, which is the limitation on the monetary amount recommended for reliance on a certificate.[127] In specifying a reliance limit, certification authorities "recommend that persons rely on the certificate only to the extent that the total amount of risk does not exceed the recommended reliance limit."[128] In so doing, the certification authority is attempting to limit liability for his or her own errors or negligence. Thus, a relying party with notice of the recommended reliance limit should not expect to recover an amount in excess of the specified amount because such reliance may be unreasonable.[129]

This ambiguous provision raises significant concerns. First, because the limit is only a "recommended" limit, questions arise as to what constitutes a reasonable reliance limit. Will the limit vary from transaction to transaction? Are there reliance limits under which it is per se unreasonable for a party to rely?

Second, it is unclear whether the "recommended" reliance limit has the legal effect of capping liability. This is because the reliance limit is a dollar amount, determined by the certification authority and the subscriber pursuant to the principles of private contracting. Nevertheless, a certification authority is by statute not liable in excess of the amount specified in the certificate as its recommended reliance limit unless he or she waives the application of this provision.[130] So, does the recommended reliance serve as a *de facto* liability cap for certification authorities notwithstanding any private agreement to the contrary? Moreover, in an open system like the Internet, is it possible for a certification authority to control—or even ascertain—potential liability when an unlimited and unknowable number of third parties rely on the same

126. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 756. As Oliver Wendell Holmes Jr. once said: "The life of the law has not been logic; it has been experience." The Common Law 1 (1881).

127. Utah Code Ann. § 46-3-103(28) (1998).

128. *Id.* § 46-3-309.

129. *See* Digital Signature Guidelines, *supra* note 16, at 65 cmt. 3.3.2. "If a relying party has notice of such a recommended limit on reliance, reliance in excess of the specified amount may well be unreasonable . . . since a relying person would have notice that the certificate was not considered suitable for transactions in excess of the specified amount."

130. Utah Code Ann. § 46-3-309(2)(b) (1998).

certificate?[131]

Third, is a "private" reliance limit arrangement between a certification authority and a subscriber even permitted? After all, certification authorities are not purely private parties, but rather governmentally licensed public officers, akin to a notary public. As such, the issue arises whether a state officer can limit its liability for its wrongdoing?

Finally, a more basic question is created by the recommended reliance limit in light of the surety bond or letter of credit that licensed certification authorities must obtain to operate. If a certification authority can be held liable for negligence up to the amount on the bond or letter of credit, then the recommended reliance limit seems duplicative.[132] Notaries public, as bonded public officials, do not issue recommended reliance limits for those who seek their services. What purpose, then, does the reliance limit serve? If the recommended reliance limit is in fact intended to cap liability, then why not simply require the certification authority to state his or her bond amount on certificates issued. If Utah's purpose was to foster confusion and uncertainty as to the liability limits of its certification authorities by creating its recommended reliance limit, it succeeded.[133]

E. Suitable Guaranty

One of the most important provisions of the Utah Act is its requirement that each licensed certification authority, other than government entities, must file a suitable guaranty with the Division.[134] It is the Division's responsibility to determine an amount appropriate for a suitable guaranty in light of the burden the requirement imposes on licensed certification authorities and the financial assurance it provides to those who rely upon the certificate's authenticity.[135] A suitable guaranty is defined as either a surety bond or an irrevocable letter of credit in an amount appropriate to protect those relying on certificates issued by the licensed certification authority.[136] This provision, like the recommended reliance limit noted above, is also fraught with deficiencies.

While the provision serves to limit the certification authority's liability for errors or negligence to the face amount of the guaranty, it does not

131. *See* Digital Signature Guidelines, *supra* note 16, at 65 cmt. 3.3.2.

132. For example, California's digital signature act holds Certification Authorities liable up to the amount on their surety bond or letter of credit, but do not require cybernotaries to post a recommended reliance limit. *See* Philip Bane, *Banking and Payment Processing on the Internet: How Should the Risk Be Allocated?,* 482 PLI/Pat 665, 679 (1997).

133. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 747 (noting that Utah's recommended reliance limit "raises more questions and concerns than it answers").

134. *See* Utah Code Ann. § 46-3-201(1)(d) (1998).

135. *Id.* § 46-3-104(3)(b).

136. *Id.* §§ 46-3-103(34); 46-3-104(3)(ii).

set a specific dollar amount.[137] By not specifying a minimal amount of financial responsibility for certification authorities, the statute fails to remedy some of the most fundamental reasons why the office of notaries public has received so little respect over the years.[138] Indeed, today's notary bond amounts are so low as to be essentially worthless,[139] assuming they are even required at all.[140] Nevertheless, the Utah Act remains silent on the issue.

Nor does Utah's law require that certification authorities carry liability insurance, which is a fundamental flaw in notary law and practice.[141] This is unfortunate, because just as errors and omissions insurance can protect notaries and the public from dire financial loss, so too can such coverage protect the certification authority and victims of the certification authority's negligence.[142] Mandatory errors and omis-

137. *Id.* § 46-3-103(34)(b).

138. Closen & Richards, *Lost in Cyberspace, supra* note 4, at 749.

139. *See* Michael L. Closen, *Why Notaries Get Little Respect*, NAT'L L.J., Oct. 9, 1995, at A23 (stating that notary bonds are "so low that [they are] useless and misleading."); Michael L. Closen & Michael J. Osty, *The Illinois Notary Bond Deception*, ILL. POL. MAG., Mar. 1995, at 13-14 (noting that the $5,000 Illinois notary bond "represents a mere symbol, left over from legislation outdated generations ago."). To illustrate:

> In the 1800s, when notary bonds were first introduced, the bond limits were typically $500 to $5,000. At that time, this was a substantial amount of coverage for a wrongful notarial act. Throughout the years, the number of notaries and notarizations grew, carriages turned into Cadillacs, and the price of consumer goods skyrocketed. Yet, the notary bond has failed to mirror the economic changes. The Illinois notary bond is a prime example of that failure. In 1913, the Illinois notary bond was $1,000. Between 1913 and 1997, the cost of consumer goods rose dramatically. If in 1913 you bought goods or services priced at $1,000, those same goods or services would cost you $16, 260, in 1997. However, Illinois, like all other states mandating a bond, failed to match the protection of the bond with escalating consumer prices. In 1986, Illinois raised the bond limit to where it currently stands at $5,000. This $5,000 limit was hardly a significant amount at the time, and eleven years later, it constitutes a completely irrelevant sum in light of the above analysis.

Michael J. Osty, *Notary Bonds and Insurance: Increasing the Protection for Consumers and Notaries*, 31 J. MARSHALL L. REV. 839, 848-49 (1998).

See also Brent Beaty, *Claims Against Notary Pubic Bonds*, AM. NOTARY MAG., January-February 1996, at 7 (illustrating the ineffectiveness of the notary bond).

140. *See* Gnoffo, *supra* note 58, at 1073 (noting that 20 states do not require notaries to be bonded).

141. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 747; Closen & Osty, *supra* note 139, at 14. *See also* Closen, *supra* note 139, at A24 (proposing that "The states should . . . mandate substantial errors and omissions insurance [for notaries].").

142. *See, e.g.*, Derrick Huckleberry, *Errors & Omissions Insurance: The Ultimate Protection!*, AM. NOTARY MAG., 1st Quarter 1998, at 1 (citing instance where notary would have been personally liable for $9,000 had she not had errors and omissions insurance). Errors and omissions insurance works like this:

> An action against the notary for misconduct triggers the claims procedure. If a notary is found liable for negligence, the E&O [errors and omissions] policy will cover the damages up to the limit on the policy. Unlike the low and practically

sions insurance for certification authorities is necessary for at least two good reasons. First, considering the magnitude of commercial transactions found in today's business environment, whatever bond amount is set by statute or by the certification authority's themselves will—judging by history—be insufficient to protect both the certification authority and the victim of the certification authority's misconduct.[143] Second, even assuming that a substantial bond amount is set for certification authorities, a bond is still insufficient to protect certification authorities themselves from financial catastrophe. This is because, unlike errors and omissions coverage, a bond is not true insurance.[144] In the event of misconduct, a bond would not protect the certification authority because the bond company will seek reimbursement from the notary for any amount they are required to pay on the bond.[145] For that reason, more financial responsibility is necessary to insure that the certification authority is fully accountable to, and fully protected from, persons claiming losses arising out of the certification authority's misfeasance. After all, shouldn't the public be able to trust the services rendered by a governmentally-licensed pubic officer?[146] Absent substantial minimum bond requirements and mandatory errors and omissions insurance for certification authorities, the office of certification authority may be doomed before it gets off the ground.[147]

> useless limits of the notary bond, an E&O policy can have a substantial higher limit, even exceeding $250,000. A further benefit of an E&O policy is that it covers the notary's legal fees incurred while defending against the claim. This is true whether or not the claimant recovers. Additionally, if the notary did negligently perform the duties of his or her office, the E&O policy will cover the resulting damages up to the limit of the policy. Though this protection is readily available today, most notaries are unaware that it even exists.

Osty, *supra* note 139, at 852.

143. *See supra* note 139.

144. *See* Closen & Osty, *supra* note 140, at 13 (noting that "a bond is not insurance.")

145. *See* Gnoffo, *supra* note 58, at 1074. Bond companies are truly the winners in this bond-for-fee arrangement. *See* Osty, *supra* note 140, at 851.

> In 1997, there were over 2.3 million notaries in the states requiring a notary bond. With the average premium for a four year bond being about $75, the money collected for these bonds is significant. The profit earned from notaries by surety companies is by no means small either. . . . [For example, in a study based on two surety companies,] results showed that, over a four year period, the two bonding companies collected over $970,000 in premiums. During that same period, the companies disbursed only $2,277.50 in claims that they could not recoup from the notaries.

Id. at 850-51.

146. Closen & Richards, *Lost in Cyberspace, supra* note 4, at 748.

147. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 748 ("Utah and other states, which set small bonds, no bonds, and no insurance or meaningful financial responsibility requirements, are signaling the direction for cybernotaries and dooming cybernotaries to positions of insignificance or serious trouble.")

F. Residency Requirement

The Utah Act requires that one must maintain an office or have a registered agent in the state for service of process to qualify as a certification authority.[148] Does this mean that a certification authority licensed by the State of Utah can authenticate a digital signature transaction that originates from a sender in California and is directed to a recipient in New York? If the Utah certification authority happens to be traveling with laptop in Illinois at the time, can the same transaction be verified? Which state law should govern such cases? In the first situation, what courts could exercise proper jurisdiction over the certification authority? If the second situation is possible, does the answer change? Even though—or perhaps because—the drafters of the Utah Act relied on notary law as a basis for many of its provisions, these questions remain unanswered.[149] This results in part due to the fact that jurisdictional issues presented in cyberspace are very different from those presented in traditional notary law and practice.[150] For instance, notaries public must generally be a resident of the state in which they act, and have authority only in their counties, parishes, or towns of residence.[151] This general rule is also true in Utah, where notaries cannot notarize documents while physically outside the State.[152] However, absent written directives addressing the geographic authority of certification authorities, the question of whether certification authorities are similarly limited remains open. The coming of electronic commerce and the authority and liability of those who participate in it has spawned a tremendous amount of debate in general.

Utah does not need to fan the flames on issues such as the geographic authority of a certification authority. Perhaps, consistent with the Utah Act's stated purpose of "establishing, in coordination with multiple states, uniform rules regarding the authentication of electronic messages," Utah could adopt a broad legislative scheme that would permit notaries to act nationally and/or internationally, much like attorneys who can be admitted to practice in another state on motion.[153] Such an

148. Utah Code Ann. § 46-3-201(1)(g) (1998).

149. *See* Biddle, *supra* note 11, at 1179 (noting that notary law and practice "appears to have been a model which was actively contemplated by the drafters of the Utah Act").

150. For a further discussion of the jurisdictional issues presented in the world of cyberspace, see generally *supra* note 6 and accompanying text.

151. Wesley Gilmer Jr., Anderson's Manual for Notaries Public § 2.10 (5th ed. 1976). *See, e.g.*, Cal. Gov. Code § 8201(a) (West 1992) (residency required); N.M. Stat. Ann. § 14-12-2(a) (Michie 1995) (residency required). In Alabama and Kentucky, notaries have countywide authority, but in Louisiana they have authority only in their parishes. *Comparison of State Notary Provisions*, Nat'l Notary Mag., May 1996, at 32.

152. *See Comparison of State Notary Provisions*, *supra* note 150, at 32 (showing that Utah notaries have statewide jurisdiction).

153. *See* Closen & Richards, *Lost in Cyberspace*, *supra* note 4, at 753.

approach is not only more consistent with the "borderless" nature of electronic commerce, but it also furthers another of Utah's stated goals "to facilitate commerce by means of reliable electronic messages[.]"[154] Regardless of the particular form of geographic authority chosen, some legislative direction is necessary in order to address the variety of questions presented by this residency requirement.[155]

G. TRUSTWORTHY SYSTEM

The Utah Act requires that certification authorities use a "trustworthy system" when fulfilling the essential requirements of his or her position.[156] A trustworthy system is defined in the statute as "computer hardware and software which: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; and (c) are reasonably suited to performing their intended functions."[157] By virtue of the Utah Act's status as "digital signature" legislation and its "key pair" security system, the statute limits the use of "trustworthy system" to encryption technology, or, more specifically, "asymmetric cryptography."[158] Because of its public key/private key configuration, many believe asymmetric cryptography is the heart of digital signature technology.[159] Without question, encryption technology is one of the most popular and secure forms of electronic transmission security procedures currently on the market. However, asymmetric cryptography, like the electronic cryptography programs that preceded it,[160] will soon be replaced by even faster and more secure anti-fraud devices. Case in point are the numerous other encryption methods which already claim to be at least as secure as the asymmetric cryptosystem, and the many others which are currently in development.[161] For this

154. UTAH CODE ANN. § 46-3-102 (1998).

155. *See, e.g.*, WASH. REV. CODE ANN. § 19.34.503 (West 1998) "Issues regarding jurisdiction, venue, and choice of laws for all actions involving digital signatures must be determined according to the same principles as if all transactions had been performed through paper documents." *Id.*

156. *Id.* § 46-3-301.

157. *Id.* § 46-3-103(38).

158. Utah defines "asymmetric cryptosystem" as "an algorithm or series of algorithms which provide a secure key pair." *Id.* § 46-3-103(1)(2). *See supra* note 19 (defining digital signature).

159. *See* DIGITAL SIGNATURE GUIDELINES, *supra* note 16, at 27 cmt. 1.3.1 (stating that asymmetric cryptography reflects "the core of digital signature technology").

160. *See supra* note 134 (discussing "private key" or symmetric cryptography).

161. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 752. One such alternative strategy is Pen Biometrics Technology ("PenOp"), which functions like the traditional paper and ink method and asserts to spread the risk in the signing of electronic documents among many baskets by requiring a hacker to compromise security features allocated among several different parties rather than among a single, vulnerable private-key holder (such as that employed in asymmetric cryptography). *See generally* Wright, *supra* note 7.

reason, many states have opted, as others have suggested, for a more open, less technologically specific, approach. For example, in the State of California a bill resembling the Utah Act was introduced in the California legislature in 1995 which proposed particular technological standards for the creation of digital signatures.[162] It soon met strong resistance from members of California's computer industry, who were concerned that any such specific protocol would stifle technological growth in the electronic communications arena.[163] As a result, the California legislature passed a much more open act which did not impose any particular technological standards.[164]

Similarly, numerous other states enacted technology neutral definitions of digital or electronic signatures,[165] as several commentators have suggested.[166] This is partly because any attempt to marshal the considerable resources necessary to unseat an already established state-approved security procedure will be difficult and time consuming, thereby decreasing competition in the market and the incentive to develop more advanced security-based systems. Our own personal experience with computers has taught us that technology advances so rapidly that computers must be updated regularly so as not to become practically obsolete. The same reasoning applies to encryption technology. Moreover, given the broad authority the Utah Act gives to the Division to make rules and regulations governing certification authorities, the law could have delegated to the Division the responsibility of adopting secure verification systems as they became available. Actually, some states have chosen to do just that.[167] Simply put, the development of security measures must not be impeded as the opportunities for fraud in electronic

162. *See* Dorney, *supra* note 19, at 158.

163. *Id.*

164. *Id.*

165. *See, e.g.*, KAN. STAT. ANN. § 60-2616 (Supp. 1998); GA. CODE ANN. § 10-12-3 (1998). *But see* FLA. STAT. ANN. § 282.72 (West 1998).

166. *See, e.g.*, Elizabeth Wasserman, *Signing On With Digital Signatures—New Laws May Allow Computer Validation*, PHOENIX GAZ., Aug. 29, 1995, at A1 (positing that security restrictions may hamper rather than promote the use of other technologies); Kennedy & Davids, *supra* note 38, at S4 ("It may be prudent, in drafting [future] digital signature legislation, also to accommodate the possibility of systems with alternative security based on methods other than public Certification Authorities and the public key repositories.").

167. *See, e.g.*, ILLINOIS ACT, *supra* note 18. The Illinois Commission provides in part:

> (a) The Secretary of State may adopt rules applicable to both the public and private sectors for the purpose of defining when a certificate is considered trustworthy . . . such that a digital signature verified by reference to such a certificate will be considered a qualified security procedure . . . . The rules may include (1) establishing or adopting standards applicable to certification authorities or certificates . . . .
>
> (b) In developing the rules, the Secretary of State shall endeavor to do so in a manner that will provide maximum flexibility to the implementation of digital signature technology and the business models necessary to support it . . . .

commerce continue to grow.[168]

H. LIMITED LIABILITY

The Utah Act limits the recovery for loss due to a negligent certification authority's conduct to direct compensatory damages.[169] Such damages do not include:" (i) punitive or exemplary damages; (ii) damages for lost profits, savings, or opportunity; or (iii) damages for pain or suffering."[170] Presumably, the drafter's intent in adopting this limited liability provision was to encourage development of the certification industry, for it was feared that exposing certification authorities to substantial liability would prohibit some certification authorities from entering the market.[171]

Limiting liability in such a manner is ill-advised for two reasons. First, it may be unnecessary to provide incentives for certification authorities to enter the industry because "profit motive" alone is one of the strongest motivations for entry. Indeed, the potential revenue that would result from the execution of thousands, if not millions, of digital signatures will likely provide sufficient encouragement for certification authorities to begin operating. Even assuming, however, that some kind of incentive is required, states can achieve equivalent or comparable results through significantly less restrictive means. For instance, perhaps the State could act as a temporary, low-cost insurer of certification authorities until the private insurance market has time to develop an appropriate and affordable insurance package.[172] This would decrease the certification authority's start-up costs, and moreover, promote the development of an industry equally as important to the formation and success of the cyberverification industry—the liability insurance market.

Second, shifting the risks of loss from the certification authority to innocent subscribers and/or relying third parties is an undesirable public policy.[173] Assume, for example, a malicious third party impersonates a

---

(c) The Secretary of State shall have exclusive authority to adopt rules authorized by this Section.

Id. at 55. In its commentary section, the Commission explains: "It is important not to adopt regulations that might unduly restrict the development and implementation of digital signature technology to facilitate electronic commerce." *Id.* at 57.

168. *See* Froomkin, *supra* note 45, at 68 ("As the amount of Internet commerce grows, the opportunities for fraud may grow unless security and authentication measures also grow.").

169. UTAH CODE ANN. § 46-3-309(2)(c) (1998).

170. *Id.* § (2)(c)(i)(ii)(iii). *But see* WASH. REV. CODE ANN. § 19.34.280(2)(c) (Supp. 1998) (including within its compensatory damages provision "lost profits, savings, or opportunity").

171. *See* Biddle, *supra* note 11, at 1192; Singer, *supra* note 30, at 734.

172. *See* Biddle, *supra* note 11, at 1192.

173. *Id.*

subscriber and, due to the certification authority's negligence, gains access to a certificate and uses it to withdraw funds from the subscriber's bank account.[174] Under the Utah Act, the certification authority would be liable only for the loss up to the suitable guaranty (or reliance limit of the certificate). This is so even though the certification authority's suitable guaranty may not be so "suitable" from the subscriber's perspective in that the coverage may be far lower than the subscriber's actual losses. Shouldn't the law protect the public from the negligent or even intentional misconduct of certification authorities rather than increase the likelihood of certification authorities acting irresponsibly. If certification authorities do not have to bear the full financial responsibility (beyond a minimal bond amount) for any losses resulting from their misdeeds, what incentive do they have to take expensive precautions against that occurrence?[175] Isn't is fair to hold the certification authority, as a public officer, more accountable to the public which it serves? After all, even notary law (which leaves much to be desired in many respects) provides that notaries may be held liable for *all* proximately caused injuries resulting from the notary's negligent, reckless, or willful conduct.[176] And this liability may even extend to the notary's employer under the common law theory of vicarious liability[177] or even the employer responsibility provisions of some state notary statutes.[178]

A better approach would be to hold certification authorities liable for all proximately caused injuries. Such an approach is beneficial not only to motivate certification authorities to obtain substantial minimum bond amounts, but more importantly to encourage certification authorities to

174. *See* Eldridge, *supra* note 22, at 1835-36.

175. Biddle, *supra* note 11, at 1192.

176. *See* Closen & Dixon, *supra* note 50, at 891. *See, e.g.,* Kork Corp. v. First Am. Title Co., 270 Cal. Rptr. 24 (Ct. App. 1990) (noting liability of notary predicated on proximately caused injury by negligent act); Tutleman v. Agric. Ins. Co., 102 Cal. Rptr. 296 (Ct. App. 1972) (noting the fact that execution of false deed was a proximate cause was enough to establish notary liability); Common Wealth Ins. Sys. Inc. v. Kersten, 115 Cal. Rptr. 653 (Ct. App. 1974) (holding notary public liable for all proximately cause injuries); Garton v. Title Ins. & Trust Co., 165 Cal. Rptr. 449 (Ct. App. 1980) (stating notary public can be held liable for all proximately caused injuries from negligently acknowledged deed).

177. *See generally* Gerald Haberkorn & Julie Z. Wulf, *The Legal Standard of Care for Notaries and Their Employers*, 31 J. MARSHALL L. REV. 735 (1998); J. Michael Gottschalk, Comment, *The Negligent Notary Public-Employee: Is His Employer Liable?*, 48 NEB. L. REV. 503 (1969); Closen, *supra* note 43, at 675-81. *See, e.g.,* Transamerica Ins. Co. v. Valley Nat'l Bank, 462 P.2d 814, 818 (Ariz. Ct. App. 1969) (holding employer liable for its notary-employees misconduct because employers practice of having a notary available was a way of improving customer relations); Garton v. Title Ins. & Trust Co., 106 Cal.App.3d 365 (Cal. Ct. App. 1980) (holding that employers can be liable for notary misconduct, including intentional official misconduct, under the ordinary vicarious liability principles); Iselin-Jefferson Fin. Co. v. United California Bank, 549 P.2d 42 (Cal. 1976) (same).

178. *See, e.g.,* IDAHO CODE § 51-118 (1996).

obtain meaningful errors and omissions insurance (which, as noted above, may be temporarily subsidized by the state). While the private insurance industry may not develop immediately, insurance companies would quickly organize risk pools of certification authorities to spread the cost of the insurance over the entire pool of certification authorities and, thus, develop an affordable insurance package.[179] Further, the insurance limit would likely be substantially higher than any bond requirements set by the parties individually. This approach would have the important benefits of fostering more trust and confidence in the electronic signature verification process, as well as protecting both the certification authority and the public from the risk of serious monetary loss.

I. REASONABLE CARE

Under the Utah Act, users of digital signatures are held to a standard of reasonable care in preserving the disclosure of their private key.[180] Given the universal goal of ensuring secure electronic commerce, this standard is entirely inadequate.[181] Is it too much to ask that the private key holder keep his private key secret?[182] The integrity of any digital signature message begins with the sender of the message—the private key holder. As such, the private key holder should be required to retain exclusive control of the private key to prevent its unauthorized use.[183] This heightened standard is more consistent with the overriding concern for fraud and theft in electronic commerce. If private key holders were informed as to their full legal responsibility for use of their keys, they would undoubtedly be more careful safeguarding their private keys.[184]

Unlike the "reasonable care" standard imposed by the Utah Act, a duty to retain "exclusive control" of the private key would, moreover, greatly increase public confidence in digital and electronic signature verifications. Furthermore, for the same reasons that insurance companies would likely insure certification authorities against errors and omis-

179. *See* Closen & Osty, *supra* note 140, at 13; Biddle, *supra* note 11, at 1192.

180. UTAH CODE ANN. § 46-3-305 (1998).

181. *See, e.g.,* UTAH CODE ANN. § 46-3-102 (Supp. 1998) (stating as one of its Act's purpose to "minimize the incidence of forged digital signatures and fraud in electronic commerce"); MINN. STAT. ANN. § 325K.02(2) (West 1998) (same); FLA. STAT. ANN. § 282.71(3) (1998) ("It is the intent of the legislature that this act: . . . Minimize the incidence of forged electronic signatures and fraud in electronic commerce."); IND. STAT. ANN. § 5-24-1-1(b)(1) (1998) (One goal of the Act is to "minimize the incidence of forged signatures and fraud in commerce.").

182. *See* Wright, *supra* note 7, at 193.

183. *See* CAL. GOV'T CODE § 16.5 (West 1998) By accepting a certificate issued by a Certification Authority, the subscriber assumes a duty to retain exclusive control of the private key and keep it confidential. *Id.*

184. *See* Closen & Richards, *Lost in Cyberspace, supra* note 4, at 753.

sions, so too would they cover private key holders against theft or loss of a private key.[185] Like errors and omissions insurance, private key insurance would have the added benefit of assuring certification authorities and their intended recipients of recovering damages in the event of loss. If digital signature verifications are to achieve the prominence and sophistication they are hoped to, a high level of accountability for private key holders is required.

J. Evidentiary Presumptions

The Utah Act, like most other digital and electronic signature laws, provides that digital signatures are as valid as paper signatures,[186] and thus can constitute a writing.[187] Under American law, the general rule when challenging the authenticity of a signature is that the signature is presumed invalid, but is subject to being rebutted in the wake of sufficient evidence.[188] However, the Utah Act obviates this traditional standard by clothing a verifiable digital signature with a presumption of validity that the challenger must counter.[189] Under Utah's legislative scheme, all digitally-signed documents are acknowledged instruments and achieve a presumption of validity.[190] Specifically, the Utah Act provides that if a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority, the court shall presume that the digital signature is that of the person listed in the certificate. In other words, it was affixed by that person with the intention of signing the message, and that the recipient had no knowledge or notice that the signer breached any duty owed to the certification authority or does not rightfully hold the private key used to manufacture the signature.[191] The effect of this provision is to shift the initial burden of proof to the private key holder or subscriber.[192] This is so even though there need be no third-party witness to the digital signing.[193]

By shifting the risk in this way, the Utah Act presumably hoped to minimize the risk that the person using the public/private key pair might be an imposter.[194] As a practical matter, however, the shifting of risk to the private key holder does not reduce such a risk, but rather

185. *Id.* at 754.
186. Utah Code Ann. § 46-3-401(1) (Supp. 1998).
187. *Id.* § 46-3-401(1).
188. *See* Closen, *supra* note 44, at 685.
189. *See* Eldridge, *supra* note 35, at 1833.
190. *See* Biddle, *supra* note 11, at 1182.
191. Utah Code Ann. § 46-3-406(3) (1998). *But see* Ga. Code Ann. § 10-12-1 to -5 (Supp. 1997) (no provision for evidentiary presumptions in the use of electronic signatures).
192. *See* Wright, *supra* note 7, at 194.
193. Utah Code Ann. § 46-3-405 (Supp. 1998).
194. *See* Wright, *supra* note 7, at 193.

transfers it.[195] Instead of placing the burden on the party challenging the digital signature, the burden is simply shifted to the private key holder to counter the presumption of validity with evidence to support its invalidity. The model contemplated by the drafters of this evidentiary presumption theory appears to have been the notary model.[196] It is regularly the case that the acts of public officers are entitled to a presumption of validity.[197] As public officers, the activities of notaries public similarly enjoy this evidentiary presumption.[198] For example, if there is a challenge to a notarization, the party objecting to the notarization must present evidence to overcome the notarization's presumption of validity.[199] After the initial showing of wrongdoing, the evidentiary burden shifts to the notary to counter with evidence to support the notarization.[200] Shifting the burden to the notary in this case is justified only after the initial showing of negligence on the part of the notary.[201] The same burden shifting rational cannot be advanced for cybernotarizations, however. This is because, unlike notary law, the digitally-signed documents are not certified individually in the presence of certification authorities—cyberspace's functional equivalent of notaries public. The physical presence of the notary to a document signing is an essential reason for its presumed reliability in legal proceedings. Thus, when the physical presence aspect is gone, the same assurances of genuineness go too. As a result, digitally-signed documents should not receive the same assurance of reliability that instruments signed in the physical presence of a notary achieve, and therefore, should not enjoy the same legal status.[202]

Furthermore, the shift in burden places an unreasonable evidentiary responsibility upon the victims of fraud.[203] Because digital signature transactions permit strangers to contract electronically, there will likely be less evidence surrounding the events of the digital signature, as compared to the traditional signing of a paper document.[204] This problem is only exacerbated by the Utah Act's minimal record-keeping re-

195. *Id.* at 194.

196. *See* Biddle, *supra* note 11, at 1180.

197. *See* Closen, *supra* note 44, at 681. *See, e.g.,* Eveleigh v. Conness, 933 P.2d 675, 682 (Kan. 1997) (noting that the presumption that a public officer has performed the duties of his or her office faithfully); *In re* Medlin, 201 B.R. 188, 192 (E.D. Tenn. 1996) ("[P]resumption that sworn public officers have properly executed their duties absent evidence to the contrary.").

198. Closen, *supra* note 44, at 681.

199. *See* Closen, *supra* note 44, at 684.

200. *Id.*

201. *See* Biddle, *supra* note 11, at 1180.

202. Biddle, *supra* note 11, at 1180.

203. *See* Biddle, *supra* note 11, at 1180-81.

204. Eldridge, *supra* note 35, at 1833.

quirement, which permits certification authorities to immediately destroy all written documentation of validly executed transactions.[205] The burden shifting is similarly unreasonable in that it is inconsistent with the standard of care required of private key holders. Utah's law requires only that private key holders use "reasonable care" to keep their private keys private. Thus, a careless private key holder who allows his private key to end up in the hands of a third party may find himself being held legally responsible for documents signed with the key, even if he did not approve the signing.[206] If a private key holder may be held liable for an unauthorized signature, and that signature is then presumed valid, the duty of care in safeguarding the private key should reflect that responsibility.

VI. CONCLUSION

The Utah Digital Signature Act fails on several levels. Many of the Act's provisions are vague, confusing, or altogether insufficient to adequately address the many new legal and policy issues presented by cyberspace. As a result, its rightful status as a "model Act" is questionable. Thus, numerous changes of the kind noted in this article are needed to prevent the undermining of such a promising future for cyberverifications.

205. *See supra* section 1.

206. *See* Eldridge, *supra* note 35, at 1833; Wright, *supra* note 7, at 193.