South Carolina Law Review

Volume 48 | Issue 2 Article 10

Winter 1997

Digital Signatures Come to South Carolina: The Proposed Digital Signature Act of 1997

Christy Tinnes

DIGITAL SIGNATURES COME TO SOUTH CAROLINA: THE PROPOSED DIGITAL SIGNATURE ACT OF 1997

I. INTRODUCTION

Digital signatures, encryption, private keys--sound like the script from "Mission Impossible?"[1] The technology wave is about to hit South Carolina. These terms are taken from legislation to be introduced in the 1997 session of the South Carolina General Assembly.[2]

The South Carolina Digital Signature Act (DSA) will enable South Carolina consumers to transact business on-line by using a unique digital signature and an encryption process that will assure them a level of security that is now lacking in Internet[3] transactions. With the digital signature process a buyer and a seller or an attorney and a client, for example, can be confident that a document executed on-line has not been altered and that all signatures are authentic.

Digital signature legislation is sweeping the nation. Utah was the first state to pass a digital signature act,[4] followed closely by Hawaii,[5] California,[6] Arizona,[7] and Washington.[8] Bills for digital signature acts were introduced last year in Michigan,[9] Georgia,[10] Rhode Island,[11] New York,[12] and Virginia.[13]

---

1. MISSION IMPOSSIBLE (Paramount Pictures 1996).

2. Draft of Bill creating the Digital Signatures Act, to be codified, if enacted, at S.C. CODE ANN. §§ 26-5-101 to -504 (unpublished draft as of Sept. 30, 1996, on file with South Carolina Senate Judiciary Committee) [hereinafter DSA].

3. The Internet currently allows anyone with a computer, a modem, and the proper software to access the World Wide Web and communicate with virtually any other participating user.

4. UTAH CODE ANN. §§ 46-3-101 to -504 (Supp. 1996).

5. S.B. 2401, 18th Leg. (Haw. 1995) (effective July 1, 1996) (allocating funding for judiciary computers in anticipation of digital signature impact).

6. CAL. GOV'T CODE § 16.5 (Deering 1996) (authorizing Secretary of State to write regulations for digital signatures by January 1, 1997).

7. ARIZ. REV. STAT. § 41-121(13) (1996) (requiring secretary of state to approve all digital signatures).

8. Act of Mar. 29, 1996, 1996 Wash. Legis. Serv. 839 (West) (passing comprehensive digital signature act similar to the Utah Act).

9. S.B. 939, 88th Leg., 1996 Reg. Sess. (Mich. 1996) (currently in Senate Committee on Technology and Energy).

10. S. Res. 621, 143d Gen. Assembly, 1995-96 Reg. Sess. (Ga. 1996) (passed in Senate and currently pending in the House Committee on Rules).

11. H.B. 8125, 1996 Leg. Sess. (R.I. 1996) (currently in House Committee on Judiciary).

12. S.B. 7420, 219th Gen. Assembly, 2d Reg. Sess. (N.Y. 1996) (currently in Senate

Digital signatures were even a hot topic at the 1996 Democratic National Convention.[14] While speaking about his state's digital signature act, Utah Senate Minority Leader Scott Howell prompted a laugh from the audience at the Democratic Leadership Council by stating, "A lot of people have been very nervous about this. . . . It's the same people who say black helicopters fly over and there's a third-world conspiracy out there and Big Brother is involved. Fortunately, we do not have very much of that in Utah. . . . [T]he new generation is much more technologically advanced."[15]

Digital signatures have the potential to be used in several aspects of everyday life and, in fact, are already being used to some extent in commerce and government. The Los Angeles County court system, for example, is testing electronic filing of legal documents using digital signatures.[16] American Express, Visa, and MasterCard have all implemented digital signature technology for on-line transactions.[17] Digital signatures integrated into Smart Cards[18] are being used to secure debit card purchases.[19] Lawmakers are granting credence for the use of this technology in electronic funds transfers, mortgage applications,[20] and virtually any contract executed on-line and requiring a valid signature. The Utah legislation provides that a digitally signed contract is "as valid, enforceable, and effective as if it had been written on paper."[21]

Obviously, the implications for attorneys are tremendous. Digital signatures will surely raise questions about the statute of frauds. Further, there are the issues of digital signature "forgery" (or some mode of security compromise) and the ability to file court documents or serve notice on-line. The American Bar Association, recognizing the effect this legislation will have

---

Committee on Judiciary).

13. H.J. Res. 129, 1996 Sess. (Va. 1996) (currently in House Committee on Rules).

14. *See* Laurie Sullivan Maddox, *Utah Demo Brags About State's Lead in Government Using Technology*, THE SALT LAKE TRIB., Aug. 29, 1996, at A10, *available in* 1996 WL 3048561.

15. *Id.*

16. See Wendy R. Leibowitz, *Technology and the Law Meet Online Commerce*, NAT'L L.J., Aug. 5, 1996, at B1 (discussing how California began testing electronic filing using digital signatures for probate court cases in May 1996).

17. *See AMEX Partners with GTE*, TREASURY MANAGER'S REP., Sept. 13, 1996, *available in* LEXIS, Legal News and Practice Library, Current News File.

18. Smart Cards are electronic cards (similar to credit cards) that contain an individually encrypted digital signature or password, known as a private key. The cards can be used at retailers with special terminals that utilize a public key to decrypt the digital signature, verifying the signature's authenticity.

19. *See The Debit Card Security Push Picks Up Speed: Expansion Efforts*, DEBIT CARD NEWS, Apr. 16, 1996, *available in* LEXIS, Legal News and Practice Library, Current News File.

20. *See Strategies Lenders Can Follow to Avoid On-Line Loan Problems*, FIN. SERVICES REP., Jan. 31, 1996, *available in* LEXIS, Legal News and Practice Library, Current News File.

21. UTAH CODE ANN. § 46-3-403(1) (Supp. 1996).

on the legal profession, issued Model Guidelines in August 1996 for states implementing their own digital signature acts.[22]

This article gives an overview of digital signature technology and describes the draft of the bill that will be introduced in South Carolina. It also discusses some of the issues that have been raised about digital signature legislation, including security, validity under the statute of frauds, case law (or lack thereof), and the scope of digital signatures worldwide.

II. HOW DOES IT WORK?

Several industries have been using electronic signatures for some time. Personal identification numbers (PINs) used for authorizing transactions at automated teller machines are a prominent example. Generally, a digital signature is a kind of electronic identification mark that becomes imposed on a message or document through the use of special software that actually encrypts the entire document. Only corresponding software with a special code can decrypt the message.

The digital signature process involves three components: the subscriber, the certification authority, and the recipient. The process is analogous to having a document notarized; a signer, a notary, and a receiver would play parallel roles.[23] The transaction begins, of course, when the subscriber executes a document. A private key (that uniquely corresponds to a public key) facilitates the initial signing. Although the term creates an image of slotted and toothed metal, a "key" is actually just a string of characters. For example, a 40-bit key is a binary number that is forty digits long. Longer, more complex keys provide better security, but the industry standard is 40-bits.[24]

The certification authority assigns keys and certifies the validity of each subscriber's digital signature, just as a notary certifies documents. Certification authorities also promulgate computerized lists that link subscribers to their public keys.[25] The lists themselves are digitally signed so that the certification authority can be investigated up a chain of higher legal accountability.[26]

---

22. *See* LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE (Info. Sec. Comm. of ABA Science & Tech. Section 1996).

23. This is based on examples given in the drafts to the ABA Model Guidelines. *See* John B. Kennedy & Shoshana R. Davids, *Bartleby the Cryptographer; Legal Profession Prepares for Digital Signatures*, N.Y. L.J., Jan. 22, 1996, at S4.

24. Elizabeth Koch & David Brenner, *How Safe is Your E-Mail? US Data Encryption Policy*, BUS. TODAY, Fall 1996, at 16, 16.

25. *See* Kennedy & Davids, *supra* note 23, at S4. Kennedy and Davids point out that the private key cannot be surmised through mere possession of the public key and mathematical skill. *See id.*

26. A. Michael Froomkin, *Innovation and the Information Environment: The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 56-57 (1996).

Forthcoming South Carolina legislation calls for the secretary of state's office to reside at the top of the chain. The secretary will supervise and license certification authorities.[27]

When a subscriber wants a recipient to rely on his digital signature, he must ask the certification authority to issue a certificate containing his public key. The subscriber is thereafter responsible for making this certificate available to potential recipients. Wider availability can be accomplished through publication in a repository of digital signatures. Special software then "reads" a document and "signs" it with a string of electronic numbers known only to the person signing the document—his private key. For longer documents, the signatory process is made easier when the document is first converted to a hash result.[28] The entire process is quite simple for the subscriber, who merely clicks an on-screen icon. The software performs the encryption process.

Once the message is received (in plain text and with a digital signature affixed), it is again a simple matter for the recipient to generate the characteristic hash result. To verify authenticity the recipient must use the public key to decrypt the digital signature and then check that the hashes are the same. Different hash marks indicate that a private key other than the one certified was used to encrypt the hash result (or document) or that the document was changed between execution and verification. On the other hand, "if everything matches, the recipient can be reasonably confident that the subscriber actually executed the document."[29]

III. DIGITAL SIGNATURE SECURITY

Security is both an advantage and a disadvantage of digital signatures. The Internet is currently an open network. Consumers purchasing goods or executing documents on-line risk having hackers pull their credit card numbers off the Internet or tamper with transmitted documents and e-mail. The FBI estimates that eighty percent of computer crime it investigates is perpetrated over the Internet.[30] The advantage is clear. Digital signatures provide essential security and allow consumers the ability to more confidently transact business on-line.

---

27. Letter from Stephen T. Draffin, South Carolina Legislative Council, to author (Sept. 10, 1996) (on file with author) [hereinafter Draffin letter].

28. A hash result is a sort of condensed version or "digest" of the original message. It is created by a mathematical algorithm in a manner that retains the uniqueness of the original message. A shorter hast result is better suited to encryption. Kennedy & Davids, *supra* note 23, at S4 n.14.

29. *Id.* at S4.

30. Froomkin, *supra* note 26, at 49 (citing DAVID ICOVE ET AL., COMPUTER CRIME: A CRIMEFIGHTER'S HANDBOOK 129 (1995)).

One disadvantage is the concern over reliability of the signatures and the uniqueness of private and public keys. The system has no inherent feature to prevent tampering with or theft of private keys. A private key is only as secure as its holder keeps it.[31] The Utah statute protects the subscriber's private key as personal property, meaning that theft or unauthorized use of a private key is subject to criminal and civil liability.[32] The South Carolina bill is expected to provide similar measures.[33]

Another concern is the security of the certification authority, which issues the public and private keys and certifies their authenticity. The certification authority innately has access to sensitive information, and confidentiality is essential. Moreover, the certification authority must have internal controls in place to regulate access to its list of public keys.[34] To ensure the necessary level of sophistication, proposed South Carolina legislation would allow only attorneys, financial institutions, title insurance companies, and certain government agencies to serve as certification authorities.[35] The South Carolina draft further would require certification authorities to undergo yearly compliance audits. Certified public accountants with expertise in computer security would conduct these audits.[36] In addition, the South Carolina draft would mandate implied warranties by the certification authority to any person reasonably relying on verification of digital signatures.[37] These warranties may not be limited or disclaimed by contract.[38] To protect the certification authority, however, the draft would charge private key owners with the responsibility of keeping their private keys confidential.[39]

To counter some of the risk, authorities can have certification security measures built into the encryption process. For example, the certificates authorizing digital signatures can be made time-sensitive by a stamping procedure.[40] This would allow a receiver to rely on the time-stamp for prioritizing documents or determining whether documents were filed within a deadline. Time coding also would allow a user to trace a document to the time it was encrypted. A time-stamp will serve as "prima facie evidence that the

31. Kennedy & Davids, *supra* note 23, at S4.

32. *See* UTAH CODE ANN. § 46-3-305 (Supp. 1996).

33. Draffin letter, *supra* note 27.

34. *See* Froomkin, *supra* note 26, at 62-63.

35. *See* DSA, *supra* note 2, § 5-201(A).

36. *See id.* § 5-202(A).

37. *See* DSA, *supra* note 2, § 5-304(A)(1); *see also* Kennedy & Davids, *supra* note 23, at S4 (discussing the ABA Draft Guidelines).

38. *See* DSA, *supra* note 2, § 5-304(A)(2).

39. *See id.* § 5-303(A).

40. *See id.* § 5-401(D)(1).

time-stamped signature took effect as of the date and time indicated in the time-stamp."[41]

As a further measure, digital signatures can be revoked.[42] The user, an immediate family member, or a business associate, agent, or employee of the user can suspend a certificate in an instant.[43] Much like the process for cancelling a credit card, the certification authority would suspend a license without confirming the identity of the person requesting the suspension.[44] Immediately upon suspension, the certification authority would be required to publish a notice in all repositories that contained the certificate.[45] An unauthorized person who requests suspension would be guilty of a misdemeanor and would incur a fine or imprisonment.[46]

Business conducted with digital signatures would also be subject to reliance limits, such as total transaction value.[47] That is, a user could set his own reliance limit when applying to the certification authority: "By specifying a recommended reliance limit in a certificate, the issuing certification authority and accepting subscriber recommend that persons rely on the certificate only in transactions in which the total amount at risk does not exceed the recommended reliance limit."[48]

IV. VALIDITY OF DIGITAL SIGNATURES

Another concern is the validity of the signature on a legal document. South Carolina's draft declares that "[a] digitally signed document is as valid as if it had been written on paper."[49] Further, the draft explicitly includes a presumption that the digital signature would be valid and binding:

> A digital signature verified using a public key is presumed to have been affixed with the intention of the subscriber to authenticate the message and to be bound by the contents of the message if:
>
> (1) the public key is listed in a certificate that is in the repository provided by the division, or a recognized repository; and
>
> (2) the certificate was not revoked, suspended, or expired at the time of signature.[50]

41. *Id.*
42. *See id.* § 5-305.
43. *See id.* § 5-305(A)(1)(a).
44. *See id.* § 5-305(A)(2).
45. *See id.* § 5-305(C)(1).
46. *See id.* § 5-305(F)(2).
47. *See id.* § 5-308(A).
48. *Id.*
49. *Id.* § 5-402(A).
50. *Id.* § 5-401(C).

The draft also discusses how the presumption could be rebutted:

> (1) by evidence indicating that a digital signature cannot be verified by reference to a certificate issued by a licensed certification authority;
> (2) by evidence that the rightful holder of the private key by which the digital signature was affixed had lost exclusive control of the private key, without violating any duty imposed by this chapter, at the time when the digital signature was affixed;
> (3) by evidence showing a lack of signature at common law; or
> (4) by a showing that reliance on the presumption was not commercially reasonable under the circumstances.[51]

V. STATUTE OF FRAUD

Article 2 of the Uniform Commercial Code requires that certain transactions be memorialized in a writing signed by the party to be charged.[52] The UCC defines signatures as "any symbol executed or adopted by a party with present intention to authenticate a writing."[53] The Official Comment indicates that the statute was "intended to make it possible for the law embodied in this Act to be developed by the courts in light of the unforeseen and new circumstances and practices."[54] Clearly, the UCC's authors anticipated technological advancement. Their broad language was meant to include future methods of "writing."

Forward-looking intent is further evidenced by current actions of the American Law Institute, the National Conference of Commissioners on Uniform State Laws, and advisers from the ABA, who are redrafting Article 2 to accommodate electronic commerce.[55] ABA Electronic Commerce Division's chairman, Thomas Smedinghoff, applauds the redraft: "Digital signatures are the key to electronic commerce . . . and the revisions to 2B will facilitate the use of digital signatures."[56] The draft is expected to be approved in July 1997. It will then be submitted to state legislatures for adaptation to existing state laws.[57]

---

51. *Id.* § 5-401(E).

52. *See* U.C.C. § 2-201 (1995).

53. *Id.* § 1-102 (39). South Carolina has adopted similar language defining a signature as including "any word or mark used in lieu of a written signature." S.C. CODE ANN. § 36-3-401(2) (Law. Co-op. 1976).

54. U.C.C. § 1-102 cmt. 1 (1995).

55. *See* Leibowitz, *supra* note 16, at B1; *see also* Marc. E. Szafran, Note, *A Neo-Institutional Paradigm for Contracts Formed in Cyberspace: Judgment Day for the Statute of Frauds*, 14 CARDOZO ARTS & ENT. L.J. 491, 498 & n.33 (1996).

56. Leibowitz, *supra* note 16, at B1 (alteration in original).

57. *See id.*

VI. CURRENT CASE LAW

Currently, no case law specifically supports a digital signature as binding. The closest the courts have come to dealing with electronic signatures have been cases concerning electronic documents such as facsimiles (faxes), telexes, telegrams and computer verifications. On these factual grounds, the courts are split.

Some courts have found that signatures transmitted electronically are binding. For example, a Pennsylvania court, in *Hessenthaler v. Farzin*,[58] held that a mailgram constituted a writing for the purpose of satisfying the statute of frauds. The *Hessenthaler* court posed the issue as whether there was "some reliable indication that the person to be charged with performing under the writing intended to authenticate it."[59] In *WPP Group USA, Inc. v. The Interpublic Group of Companies, Inc.*,[60] a New York court held that the subscription requirement of the statute of frauds was met by an unsigned legend on a fax. A New Jersey court, in *Spevack, Cameron & Boyd v. National Community Bank of N.J.*,[61] found that a unique bank account number sent on-line is as complete a signature as a depositor's written name. The *Spevack* court noted: "In this computer age the use of numbers as a means of identification has become pervasive. Indeed, numbers are more readily recognized and handled than signatures. . . . The 'signature' accurately identified the payee . . . ."[62]

Other courts, however, have refused to recognize a binding power in electronic documents or communications. One court refused to allow reliance on a telex sent by a bank.[63] Another held that a computer assigned tracking number issued in response to a telephoned offer to buy did not constitute acceptance.[64] Still a third held that a name on a telegram did not constitute a signature under the statute of frauds.[65]

Fourth Circuit courts have addressed electronic communication in the area of service of process and the filing of court documents. A federal district court in North Carolina determined that service by fax does not meet the require-

58. 564 A.2d 990 (Pa. Super. Ct. 1989).

59. *Id.* at 993.

60. 644 N.Y.S.2d 205 (N.Y. App. Div. 1996).

61. 677 A.2d 1168 (N.J. Super. Ct. App. Div. 1996).

62. *Id.* at 1169.

63. *See* Quatar Nat'l Navigation & Transp. Co., Ltd. v. Citibank, N.A., No. 89 Civ. 464 (CSH), 1996 WL 54382 (S.D.N.Y. Feb. 9, 1996).

64. *See* Corinthian Pharm. Sys., Inc. v. Lederle Lab., 724 F. Supp. 605, 610 (S.D. Ind. 1989).

65. *See* Pike Indus., Inc. v. Middlebury Assocs., 398 A.2d 280, 282 (Vt. 1979).

ments of Federal Rule of Civil Procedure 5(b).[66] The court decided to leave the matter to the rulemakers:

> The decision today that the new technology of fax transmissions does not constitute service under Rule 5(b) is not a criticism of the technology. Rather, it is recognition that this and related new technology would be better integrated in to the civil rules through the collegial process of a rules committee, which can obtain and consider a broader range of suggestions and opinions.[67]

In a more recent case, a district court in South Carolina declined to adopt the "receipt rule"[68] in a removal action because, among other reasons, formidable questions regarding electronic communications would be raised.[69] The court pointed out that "[c]ourtesy copies, faxes, and e-mail delivered to whomever picks up the mail, receives the fax, or turns on the computer is not an inherently fair method to put a defendant on notice of the date on which the removal time period has begun."[70]

The Fourth Circuit, however, does permit filings by fax. In accordance with the Federal Rules, which allow electronic filings subject to local rules,[71] if an attorney files by fax, he does not have to file the original signed paper.[72]

VII. SCOPE

The process of digital execution has international ramifications. The United Nations Commission on International Trade Law (UNCITRAL) has proposed legal guidelines for uniformity in international electronic commerce.[73] The ABA's Section of Science and Technology has worked with the

---

66. *See* Salley v. Board of Governors, 136 F.R.D. 417 (M.D.N.C. 1991); *see also* FED. R. CIV. P. 5(b) (discussing service and filing of pleadings and other papers).

67. *Salley*, 136 F.R.D. at 420 n.2.

68. "The 'receipt rule' requires that a defendant must remove a state action to federal court within thirty days of receipt of a copy of the initial pleadings, without regard to whether service has been effected." Bowman v. Weeks Marine, Inc., 936 F. Supp. 329, 332 (D.S.C. 1996).

69. *See id.* at 339.

70. *Id.* at 342.

71. *See* FED. R. APP. P. 25(a)(2)(D).

72. *See* FED. R. APP. P. 25, Local Rule 25(b)(1) (suggesting that attorneys fax to a printing service in Richmond, which will accept papers by fax and file them with the court--filings can be faxed to the clerk only in emergency situations with advance permission.) Although Federal Rule of Civil Procedure 5(e) allows filing by facsimile or other electronic means if authorized by the local rules, the South Carolina district court has not provided such a rule.

73. *See* Richard Hill & Ian Walden, *The Draft UNCITRAL Model Law for Electronic Commerce: Issues and Solutions*, 13 COMPUTER LAW., Mar. 1996, at 18, 18.

notarial bars of Western European countries, Mexico, the Province of Quebec, and the United States State Department to create CyberNotaries that would electronically certify transactions under United States and foreign law.[74]

The broad application of this technology has created some controversy. Encryption software is considered a munition under the International Traffic in Arms Regulations (ITAR).[75] As such, exporting encryption software is banned under ITAR.[76] In one instance, the United States government investigated an encryption software inventor for twenty-eight months because he made software available to citizens knowing that they would post it on the Internet where foreign nationals could access it.[77] The charges, however, were eventually dropped. In another case the State Department advised a cryptographer to obtain a license from the State Department before publishing a scientific paper describing his cryptographic algorithm.[78] The State Department later withdrew its order. Before worldwide digital signatures can be effective, these concerns must be addressed.

VIII. CONCLUSION

South Carolina is ready for digital signature technology. As more and more commerce is carried out on the Internet the need for greater security is essential. Digital signatures and electronic commerce promote efficiency and economy of data transfer and document execution.

Certainly, there are issues yet to be addressed. Private key security and public/private key pairing confidentiality are the most pressing matters. The proposed South Carolina legislation has foreseen these concerns and provided that only certain sophisticated groups may be certification authorities who can assign pairs. These certification authorities must undergo yearly compliance audits to ensure that they are following specified internal controls. Also, a digitally executed document is time-sensitive and subject to reliance limits set by its author. In addition, a private key may be revoked at any time at the option of its owner.

---

74. *See* Michele C. Kane, *Addressing Implications of Digital Signatures*, NAT'L L.J., July 10, 1996, at D13.

75. *See* 22 C.F.R. § 121.1 (1996).

76. *See id.* § 121.8. The statutory authority for ITAR, *id.* § 120.1—130, is the Arms Export Control Act, 22 U.S.C. § 2778 (1994). *See* Edward J. Radlo, *Legal Issues in Cryptography*, 13 THE COMPUTER LAW., May 1996, at 1, 4; *see also* William J. Cook, *Export Problems Deliver Cryptic Message about Encryption*, CHICAGO LAWYER, Sept. 1996, at 74, 74.

77. *See* Radlo, *supra* note 76, at 7 (discussing the federal grand jury investigation of Phil Zimmermann).

78. *See* Bernstein v. United States Dep't of State, No. C-95-0582 MHP, 1996 WL 730283 (N.D. Cal. Dec. 9, 1996); Bernstein v. United States Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996), *cited in* Radlo, *supra* note 76, at 7 (discussing reasons why State Department withdrew its order).

Digital signatures also bring up the question of the writing requirement under the statute of frauds. The South Carolina DSA explicitly sets out a presumption that a document executed with a digital signature is valid as if written on paper. Currently, the American Law Institute and the National Conference of Commissioners on Uniform State Laws are in the process of redrafting Article 2 of the UCC to accommodate electronic commerce.

There is very little case law in this emerging area of electronic commerce. Most cases deal with faxes or telexes. Some courts have addressed electronic communication on a limited basis by allowing filing via computer. Digital signature technology will likely lead to a whole new area of case law, and the South Carolina courts must be equipped to meet the demand.

The American Bar Association and state legislatures have recognized the need for this legislation. The drafters of Article 2 have anticipated the trend toward electronic commerce. Even the United Nations has addressed cryptology issues. The General Assembly should be commended for keeping South Carolina looking to the future with this technologically advanced legislation.

Christy Tinnes