Washington's Electronic Authentication Act: Eliminating Legal Uncertainties Through Default Rules

THOMAS G. MELLING*

A uniform system of managing information technology and computer networks is needed to cope with the impact of the information age. It is the responsibility of the legislature to manage this technology and to change or amend the statutes as needed.[1]

Digitalization of information and communications is causing both subtle and dramatic changes in our society. Computers and other new digital technologies make communications faster and more efficient, and lower the cost and increase the availability of information. They also may pose problems for existing laws, many of which were adopted or promulgated long before the digital era. Legal articles frequently raise the question whether existing laws are outdated and unsuited for the

* J.D., Stanford Law School, 1994; B.A., Brown University, 1989; Associate, Hillis Clark Martin & Peterson, P.S. E-mail: tgm@hcmp.com. The author is a member of the Washington Digital Signature Implementation Task Force and is a representative of the Business Law Section of the Washington State Bar Association to the Information Security Committee of the American Bar Association. The views expressed in this paper are his own.

1. It's In The Cards, Inc. v. Fuschetto, 535 N.W.2d 11, 15 (Wis. Ct. App. 1995).

issues created by digital technologies, or whether such laws are satisfactory and do not need to be modified.[2]

To date, changes to existing laws have been mostly academically debated, but not enacted. One exception is in the field of electronic commerce. The National Conference of Commissioners on Uniform State Law (NCCUSL) will soon produce Article 2B of the Uniform Commercial Code.[3] This new UCC article, upon adoption by individual states, will govern all transactions in software, and the licensing of information.[4] The most significant legislative activity, however, has occurred in the area of digital signatures. At least 12 states have enacted some form of digital signature legislation, which provide a framework for the authentication of computer-based transactions and communications. An equal number of states are considering legislation or will likely enact some form of legislation soon.[5]

Although digital signature legislation has been adopted or is being considered by many states,[6] some legal commentators question its necessity and assert that such legislation may be more harmful than beneficial. Brad Biddle presents these arguments in his article "Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace."[7] According to Biddle, digital signature legislation should not be enacted for two reasons. First, it is unnecessary

---

2. *See, e.g.*, Wendy R. Leibowitz, *Personal Privacy and High Tech: Little Brothers Are Watching You*, NAT'L L.J., April 7, 1997, at B16 (discussing whether privacy law can "cope" with the Internet); Craig J. Blakeley, *No Bliss Yet for Online Calls*, NAT'L L.J., Feb. 3, 1997, at C1 (discussing regulation of long-distance telephone calls over the Internet); Wendy R. Leibowitz, *The Internet Blunts TM Protection*, NAT'L L.J., Feb. 10, 1997, at B1 (discussing the "problems arising from the application of trademark law to the Internet"); Stuart D. Levi & Robert Sporn, *Can Programs Bind Humans to Contracts*, NAT'L L.J., Jan. 13, 1997, at B9 (discussing how "'intelligent agents' capable of shopping the Web and entering 'click wrap' pacts wreak havoc with aged contract and agency laws").

3. *See* A. Brian Dengler, *UCC Article 2B on the Fast Track: New Commercial Rules Around the Corner*, 4 INTELL. PROP. STRATEGIST, Jan. 1997, at 6.

4. The most current draft of Article 2B can be found online at Uniform Commercial Code Article 2B Revision Home Page (visited Oct. 6, 1997) <http://www.law.uh.edu/ucc2b>.

5. A state-by-state summary of legislation is available online at McBride Baker & Coles, *Summary of Legislation and Other Initiatives Relating to Digital Signatures, Electronic Signatures and Cryptography* (visited Oct. 6, 1997) <http://www.mbc.com/ds_sum.html>. The State of Massachusetts also has a summary online at Commonwealth of Massachusetts, Information Technology Division Legal Department, *The Citizens Would Rather Be On-Line Than In Line* (visited Oct. 6, 1997) <http://www.magnet.state.ma.us/itd/legal>.

6. For a summary of state and federal initiatives, see (visited Feb. 26, 1998) <http://www.mbc.com/ds_sum.html>.

7. C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, 34 San Diego L. Rev. 1225 (1998).

because the legal uncertainties and risks associated with the use of digital signatures can be solved by parties through private contracts. Moreover, argues Biddle, the "open PKI"[8] system is based upon business models that cannot absorb the liabilities from fraudulent use of digital signatures. Only through private contracts, or a "closed PKI" system, will digital signatures be feasible. Second, Biddle argues that digital signature legislation will harm the infant electronic commerce market by legislating market winners and will expose consumers to unreasonable risk and liabilities.

This Article responds to Biddle's arguments against digital signature legislation. The focal point for the response is the Washington Electronic Authentication Act.[9] Although the Washington Act is similar to the Utah Digital Signature Act[10] and the "open PKI" system described by Biddle, new amendments to the Washington Act avoid some of the problems and concerns raised by Biddle. Part I explains the history of the Act's adoption, and details some of the amendments that make it unique. Part II rejects most of Biddle's arguments about digital signature legislation. Because the Washington Act creates default background rules that may be altered by private contract, there is little or no risk that the Washington Act will legislate market winners, or distort the electronic commerce market. However, Part II agrees that digital signature legislation, including the Washington Act, fails to adequately protect consumers. Although Biddle overstates the risk, the Washington Act and other digital signature legislation should be amended because even if the risk is not high, consumers' perceptions of the risk will impede their use of digital signatures. Finally, Part II challenges Biddle's conclusion that a closed PKI system will ultimately

---

8. "Open PKI" refers to a type of public key infrastructure ("PKI"). According to Biddle:

> The Utah Act and its progeny, and the ABA Guidelines, are premised on an "open system" or "open loop" model of PKI. The open PKI model envisions that subscribers will obtain a single certificate from an independent third-party CA which certifies that subscriber's identity. [Subscribers] will then use that certificate to facilitate [all] transactions with potentially numbers merchants and/or other individuals.

Biddle, *supra* note 7, at 1234-35. As discussed in Part I *infra*, this Article uses a similar definition of an "open PKI" system, but does not assume that a subscriber will obtain only a single certificate. Each person or entity may obtain multiple certificates for the types of transactions in which they will be creating a digital signature.

9. WASH. REV. CODE §§ 19.34.010 - 19.34.903 (Supp. 1997).

10. UTAH CODE ANN. §§ 46-3-101 - 46-3-504 (Supp. 1997).

prevail over an open PKI system. Over time both open and closed systems will be used in the marketplace. If digital signatures become the preferred means of conducting electronic commerce, especially with consumers, it is likely that some type of open PKI system will be widely accepted.

I. WASHINGTON'S ELECTRONIC AUTHENTICATION ACT

This article presumes that the reader is familiar with the basic technology of digital signatures and the relationships between the subscriber, certification authority, repository, and relying party in the process of creating and verifying a digital signature.[11] To understand the reasons for supporting the Washington Act, however, it is necessary to summarize its key provisions. In addition, this Part details the significant new amendments to the Washington Act, which help resolve some of the potential problems.

The Washington Electronic Authentication Act, originally enacted in April 1996, closely followed the model established by the Utah Digital Signature Act. Washington's legislature, however, chose to delay implementation of the Washington Act until January 1, 1998,[12] and to convene a task force to examine the business and legal issues associated with digital signatures. Members of the task force included government officials, lawyers, and representatives from a wide array of business interests, including banks, the insurance industry, and software and computer companies. The task force met throughout 1996 and into early 1997, and ultimately recommended several significant amendments to the original Act. Although the task force and other individuals who became involved in the amendment process did not agree on all modifications, a compromise was reached, and the Washington legislature passed Senate Bill 5308 during the 1997 legislative ses-

---

11. For more information about digital signatures, see Information Security Committee, Electronic Commerce and Information Technology Division, Section of Science and Technology, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, 1996 A.B.A. SEC. SCI. & TECH. L. REP., at 3-17 (visited Mar. 9, 1998) <http://www.abanet.org/scitech/ec/isc/dsgfree.html>; A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 51-67 (1996); ONLINE LAW: THE SPA'S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET (Thomas J. Smedinghoff ed., 1996).

12. WASH. REV. CODE § 19.34.901 (Supp. 1997).

sion.[13] The Washington Secretary of State, with consultation from the task force, has also implemented regulations for the Act.

The rules established in the Washington Act can be generally categorized as follows: (1) the licensing of certification authorities; (2) the issuance, suspension and revocation of certificates; (3) duties, warranties, and obligations of licensed certification authorities, subscribers, and relying third parties; and (4) rules regarding the validity of digital signatures.

Under the Act, certification authorities do not need to obtain a license to conduct business.[14] Although the decision whether or not to obtain a license is voluntary, licensed certification authorities enjoy several benefits under the Act. Their liability is limited in certain circumstances.[15] Also, the Act establishes a presumption that a digital signature verifiable to a public key listed in a valid certificate issued by a licensed certification authority satisfies formal requirements of a signature.[16] The Act is silent as to whether a digital signature associated with an unlicensed certification authority satisfies the requirements of a signature. To obtain a license, a certification authority must (a) itself have been issued a certificate which is published in a recognized repository, (b) employ operative personnel who have demonstrated knowledge of the requirements of the Act and who have not been convicted of fraud or a recent felony, (c) file a suitable guaranty with the Washington Secretary of State, (d) use a trustworthy system, and (e) have an office in the state of Washington.[17]

The licensing requirements are potentially an important aspect of an open PKI system. An open system is only viable if relying parties believe certification authorities are trustworthy, and that the certification authority has properly bound the subscriber to the public key listed in

---

13. Senate Bill 5308 was enacted on April 15, 1997. S. 5308, 55th Leg., 1st Reg. Sess. (Wash. 1997). For a copy of the Act (as amended) as well as the new regulations implementing the Act, see (visited Feb. 26, 1998) <http://www.wa.gov/sec/corps/digsig.htm>.

14. The Washington Act does not apply to unlicensed certification authorities, except as specifically provided. WASH. REV. CODE § 19.34.100(7) (Supp. 1997). Furthermore, the Act states that the licensing provisions of the Act "do not affect the effectiveness, enforceability, or validity of any digital signature . . . ." WASH. REV. CODE § 19.34.100(6) (Supp. 1997).

15. *See infra* text accompanying notes 23-24.

16. WASH. REV. CODE § 19.34.300 (Supp. 1997).

17. WASH. REV. CODE § 19.34.100 (1996).

the certificate. The licensing requirements attempt to provide some assurances to relying parties that the certification authorities are, in fact, trustworthy. It is likely, however, that the reputation and brand name of a certification authority will be far more important to a relying party than proof that a certification authority has obtained a license from the Washington Secretary of State.[18] In addition to licensing, other approaches are being considered to address the reliability of certification authorities and certificates. The Information Security Committee of the American Bar Association is working to develop a rating system for certificates, much like a bond rating system.[19] It is unclear whether such a rating system will ultimately prove feasible, however, because of the large number of variables that can affect the reliability of certificates. South Carolina is considering legislation that "would allow only attorneys, financial institutions, title insurance companies, and certain government agencies to serve as certification authorities."[20]

The Act prescribes several conditions that must be satisfied before a licensed certification authority may issue a certificate. These conditions include confirmation by the certification authority that: (i) the subscriber is the person to be listed on the certificate, (ii) the information in the certificate is accurate, (iii) a prospective subscriber rightfully holds a private key corresponding to the public key to be listed in the certificate, and (iv) the certificate provides information sufficient to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate would be listed.[21] The certificate may also include a "reliance limit," which is "the monetary amount recommended for reliance on a certificate . . . ."[22]

If the certification authority satisfies the above requirements, the certification authority is not liable for losses caused by reliance on a false or forged digital signature of a subscriber.[23] If, however, the licensed certification authority fails to satisfy these requirements, the certification authority is liable up to the amount of the recommended reliance limit specified in the certificate.[24]

---

18. Mike Rodin, *Digital Signatures - Get Ready 'Cause Here They Come,* 22 BUS. L. SEC. NEWSL. 3, at 4 (1997).

19. Information Security Committee, Section of Science and Technology, *Certificate Policy and Certification Practices Framework,* 1997 A.B.A. SEC. SCI. & TECH. INFO. SEC. COMMITTEE (visited Mar. 9, 1998) <http://www.abanet.org>.

20. Christy Tinnes, *Digital Signatures Come to South Carolina: The Proposed Digital Signature Act of 1997,* 48 S.C. L. REV. 427, 431 (1997).

21. WASH. REV. CODE § 19.34.210 (Supp. 1997).

22. WASH. REV. CODE § 19.34.020(28) (1996).

23. WASH. REV. CODE § 19.34.280(a) (1996).

24. WASH. REV. CODE § 19.34.280(2)(b) (1996).

Upon acceptance of a certificate, the subscriber "assumes a duty to exercise reasonable care to retain control of the private key."[25] The subscriber is released from this duty if the certificate expires or is revoked. If a subscriber does not exercise reasonable care, and loses control of his or her private key, such subscriber bears unlimited liability, provided, however, that the recipient of a digital signature assumes the risk that a digital signature is forged if reliance on the digital signature is not reasonable under the circumstances.[26] For example, it may not be reasonable to rely upon a purchase order for a product costing $3,000 if the reliance limit in the certificate is only $1,000.

A digital signature satisfies the formal requirements of a signature if the digital signature is verifiable by reference to the public key listed in a valid certificate issued by a licensed certification authority.[27] The Act also establishes several presumptions in the adjudication of disputes. If a digital signature can be verified to the public key listed in a valid certificate, it is legally presumed the digital signature is the digital signature of the subscriber listed in the certificate.[28] In addition, any digitally signed message satisfies the evidentiary requirements of an original.[29]

Most of the provisions described above are similar to the Utah Digital Signature Act. However, recent amendments to the Washington Act make it unique in several respects. A majority of the members of the task force preparing the amendments and other interested parties believed that the acceptance of a digital signature should be voluntary. Several provisions of the Washington Act address this concern. The Act provides that nothing precludes the recipient of a digital signature from establishing conditions under which the recipient will accept the digital signature.[30] It also provides that any recipient or other person asked to rely on a digital signature is not obligated to accept a digital signature

25. WASH. REV. CODE § 19.34.240(1) (1996).
26. WASH. REV. CODE §§ 19.34.240(1), 19.34.310 (1996).
27. WASH. REV. CODE § 19.34.300 (Supp. 1997).
28. WASH. REV. CODE §§ 19.34.240(1), 19.34.350(3) (1996).
29. WASH. REV. CODE §§ 19.34.320, 19.34.330 (Supp. 1997).
30. WASH. REV. CODE § 19.34.320 (Supp. 1997). Section 19.34.320 of the Revised Code of Washington also provides that a digitally signed message shall not be deemed to be an instrument under Washington's Uniform Commercial Code unless all the parties to the transaction agree. *Id.*

or to respond to an electronic message containing a digital signature, except for digital signatures from courts.[31] While many commentators have been critical of digital signature legislation because of the liability exposure to subscribers, there has been less debate about the implications of forcing people to use this new technology. The Washington Act should help resolve such concerns.

The new amendments also explicitly provide that the Act's provisions may be modified by agreement, except that a person may not disclaim responsibility for lack of good faith.[32] Thus, nothing prevents parties, including a licensed certification authority, from contractually creating a closed system. For example, parties may create a hybrid system that uses some of the default rules provided by the Act, but modify other provisions to suit the parties' particular needs.

The Washington Act is similar but not necessarily identical to the open PKI model described by Biddle. The Washington Act is an open system because the legal presumptions and obligations apply to any certificate issued by a licensed certification authority. Biddle's definition of an open system, however, "envisions that subscribers will obtain a single certificate from an independent third-party CA which certifies that subscriber's identity."[33] Although it is possible for a subscriber to conduct all transactions using only one certificate under the Washington Act, its seems more likely that subscribers will use more than one certificate depending upon the type of transaction. For example, a subscriber may have a low level certificate to sign electronic mail or purchase small products. They may obtain transactional certificates for larger transactions.[34]

II. A DEFENSE OF OPEN PKI LEGISLATION

The Internet and other open networks create a tremendous opportunity for electronic commerce. The disadvantage of an open network, however, is that communications and transactions are generally unsecure. The movement to enact digital signature legislation has arisen from efforts to resolve these security problems. While a public key infrastructure provides a framework to authenticate computer-based transactions

---

31. The phrase "accept a digital signature" means to verify a digital signature or take an action in reliance on a digital signature. WASH. REV. CODE § 19.34.020(2) (Supp. 1997).

32. S. 5308, 55th Leg., 1st Reg. Sess., § 34 (Wash. 1997).

33. Biddle, *supra* note 7, at 1234.

34. A transactional certificate is a "certificate incorporating by reference one or more digital signatures," but which use only one for individual transactions. WASH. REV. CODE § 19.34.020(37) (Supp. 1997); *see also* Froomkin, *supra* note 11, at 63-65.

and communications, most scholars agree that the existing laws that would govern an open PKI system are uncertain.[35] Digital signature legislation such as the Washington Act establishes clear rules regarding the validity and enforceability of digital signatures, as well as the liabilities and obligations of the subscriber, certification authority, repository, and relying party.

In his arguments against the adoption of open PKI legislation, Biddle does not assert that the existing laws that would govern an open PKI system are clear. Rather, Biddle argues that existing legal uncertainties can be resolved through contracts—that is, a closed PKI system in which the subscriber, relying party, and certification authority contractually establish rules governing the enforceability of digital signatures and the allocation of liability. Moreover, he asserts that open PKI legislation is not viable because it creates "immense" liabilities that cannot and will not be absorbed by affected parties.[36] The harm of implementing such legislation, according to Biddle, is the risk of "profoundly distorting an infant market," which may impede the growth of electronic commerce, and "lock-in" laws harmful to consumers.[37] This Section examines these arguments, responding first to the arguments about the potential of an open PKI legislation. The second half analyzes whether a closed PKI system will ultimately prevail, and discusses some of the shortcomings of a system that must rely solely on private contracts.

---

35. *See* Froomkin, *supra* note 11, at 84. The draft Report by the Internet Law & Policy Forum concludes:

> [T]here is no doubt that the specter of liability for breach of contract and for negligence significantly deter the entry of CAs into the market. At this point there are no efficient markets for insurance to spread risk through the industry—meaning that CAs face meaningful unquantifiable risks of large losses. Placing risk of loss on CAs when CAs act reasonably would likely make those risks untenable, posing a grave threat to the development of the CA industry.

The Role of Certification Authorities in Consumer Transactions: A Report of the ILPF Working Group on Certification Authority Practices (draft), 1997 INTERNET LAW & POLICY FORUM, at 20 (on file with author) [hereinafter *Role of Certification Authorities*]. *See also* U.N. COMMISSION ON INT'L TRADE LAW, REPORT OF THE WORKING GROUP ON ELECTRONIC COMMERCE ON THE WORK OF ITS THIRTY-FIRST SESSION, at 7, U.N. Doc. A/CN.9/437 (1997) (English version, on file with author) ("[T]he absence of a legal regime for digital and other electronic signatures might pose an impediment to electronic transactions effected through electronic means.").

36. Biddle, *supra* note 7, at 1226.

37. *Id.* at 1226.

A. Avoiding the Potential Harms

1. Uniform Default Rules

The primary purpose of the Washington Act is to establish clear default rules governing transactions involving digital signatures. While the Utah Act does not address whether it may be modified, Washington's Act specifically provides that rules regarding the allocation of liability may be contractually altered by the parties.[38] For example, a certification authority may be licensed in Washington, and still be part of a closed system that contractually controls the use of digital signatures and reallocates the risk of loss between the subscriber, relying parties, and the licensed certification authority. Thus, the Act does not interfere with the development of closed PKI systems.

The ability to contractually alter default rules is an important principle of commercial law.[39] Freedom of contract is a basic philosophy of the Uniform Commercial Code, and should be included in any digital signature legislation that creates rules governing the parties' obligations and liabilities.[40]

Furthermore, although the default rules are only applicable to *licensed* certification authorities, there is nothing in the Act that prevents an unlicensed certification authority from issuing certificates as part of a closed PKI system. Some commentators have argued that the Washington Act may force all certification authorities to obtain a license because only licensed certification authorities receive limited liability under the Washington Act. This argument is flawed, because, as Biddle correctly

---

38. WASH. REV. CODE § 19.34.350 (Supp. 1997). This provision was adopted from Section 34 of the 1997 Amendments, which provides:

> The effect of this chapter may be varied by agreement, except:
>
> (1) A person may not disclaim responsibility for lack of good faith, but parties may by agreement determine the standards by which the duty of good faith is to be measured if the standards are not manifestly unreasonable; and
>
> (2) As otherwise provided in this chapter.

S. 5308, 55th Leg., 1st Reg. Sess., § 34 (Wash. 1997). The only provisions of the legislation that may not be altered are the certification authorities' warranties about the contents of a certificate. *Id.*

39. Raymond T. Nimmer, *UCC Revision: Information Age in Contracts*, 29 A.L.I.-A.B.A. 17 (1996).

40. Section of Business Law Ad Hoc Task Force on Electronic Contracting, *National Conference of Commissioners on Uniform State Laws Drafting Committee on Electronic Contracting-Proposal on Scope of Model [Electronic Contracting] Act*, 1996 A.B.A. SEC. BUS. LAW AD HOC TASK FORCE ON ELECTRONIC CONTRACTING (visited Mar. 9, 1998) <http://www.abanet.org>.

argues, parties in a closed PKI system can not only limit the scope of their liability, but can further establish rules governing the allocation of risk and the validity of digital signatures.[41] If Biddle is correct that a closed PKI model will ultimately prevail, we should see a robust unlicensed certification authority market develop in the state of Washington even though only licensed certification authorities enjoy the liability limitations under the Act.

2. *Correcting the Risk of Potential Consumer Liability*

Biddle's second argument, which has been raised by other legal observers,[42] is that open PKI legislation shifts liability exposure to consumers. Under the Washington Act, a subscriber has unlimited liability if the subscriber does not exercise reasonable care to protect his or her private key.[43] To dramatize the potential implications of this provision, Biddle gives the example of a "Grandmom" who does not exercise reasonable care, incurs $25,000 of liability, and loses her house.[44] While this example raises concerns, the actual risk to consumers is probably small. Most cases of fraud will very likely arise from theft of a consumer's key. And if a consumer's private key is stolen, the determination of whether the consumer was negligent will be decided by a judge or jury and would probably require egregious facts. In addition, the subscriber is not liable under the Washington Act if reliance upon the certificate is not reasonable.[45] For example, Grandmom's key would probably have a relatively small reliance limit—she would most likely use it to order groceries at the local store for delivery rather than to purchase thousand dollar consumer goods. It is unlikely that she would be liable for any contract greater than the reliance limit in her certificate.

---

41. Biddle, *supra* note 7, at 1227.
42. *Role of Certification Authorities*, *supra* note 35, at 21. The Report concludes:
> We believe that consumer protection is an integral step in encouraging the use of digital signatures . . . . We are concerned that unlimited losses could be a major disincentive for consumers to participate in the system. Thus, we suggest that consideration be given to limiting consumer liability even in the situation where a consumer does not act reasonably.

Id.
43. *See supra* text accompanying note 25.
44. Biddle, *supra* note 7, at 1236.
45. WASH. REV. CODE § 19.34.310 (Supp. 1997).

Even though the risk to consumers is probably small, there are at least two reasons why consumer liability should be limited. First, simply the perception of risk could drastically affect consumers' use of digital signatures. Consumers' fear about credit card security, not actual risk, has severely limited the growth of electronic commerce.[46]

Second, digital signature legislation, like other commercial laws that establish default rules, should reflect the expectations of the parties. Raymond T. Nimmer, the NCCUSL Reporter for Article 2B, considers this to be a fundamental principle of contract law:

> Uniform contract laws do not regulate practice. They seek to sustain and facilitate it. The benefits of codification lie in defining principles consistent with commercial practice which, because of their codification and their relevance to actual practice, can be relied on and are readily discernible and understandable to commercial parties.[47]

The potential of unlimited liability from the loss of a private key is not consistent with consumers' expectations or existing law.[48] Under the Electronic Fund Transfer Act, consumers' liability is capped in most cases at $50 even if the consumer did not act with reasonable care.[49]

If the Washington Act is amended so that a subscriber's liability is limited to $50, a large proportion of the risk of liability would fall upon the relying party, because the certification authority's liability is limited to the reliance limit in the subscriber's certificate. This loss allocation would be appropriate in a merchant-consumer transaction, because the merchant is best able to spread the cost of fraud to all consumers through pricing.[50] This loss allocation in merchant-merchant transactions may be less important, suggesting that an amendment limiting a subscriber's liability for the negligent loss of a private key should apply only to consumers, not merchants.

---

46. *See, e.g.*, Elizabeth Weise, *Promoters Try to Ease Shoppers' Fears of Credit Card Fraud on the Internet*, BUFF. NEWS, Jan. 22, 1997, at A4.

47. Nimmer, *supra* note 39.

48. C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L. REV. 1143, 1170 (1996).

49. 15 U.S.C. § 1693(g) (1996).

50. *Role of Certification Authorities*, *supra* note 35, at 20-21. The report believes that allocating the consumer/subscriber's liability to merchants is analogous to laws governing mail orders and telephone-based transactions in which merchants bear the risk. *Id.*

B. Open PKI vs. Closed PKI: Predicting the Winner

Biddle argues that a closed PKI model, rather than an open PKI model, "will be the winner in the marketplace."[51] His argument is based on the following assumption: Subscribers using a single certificate in an open PKI system create the potential of enormous liabilities from fraud, and parties will be unable to risk, and unwilling to incur, these liabilities. There are several reasons why this assumption should be questioned.

Under the Washington Act, subscribers can obtain more than one certificate, and each certificate can limit its use to specific types of transactions. For example, the certificate can limit the monetary size of the transactions for which it is valid.[52] It may also be possible to limit the types of recipients who are entitled to rely upon the certificate.[53] Consequently, parties can manage their potential liability exposure under the Washington Act just like parties in a closed system.

Digital signature fraud may not be overwhelming or rampant. To illustrate the potential for fraud, Biddle cites examples of MasterCard and VISA losing over $1 billion per year from fraud and the City of Los Angeles expending $131 million in fraudulent real estate document filings in a twenty-seven month period. Most commentators, however, have concluded that private keys are much more secure than credit cards.[54] Unlike an owner of a credit card who must disclose his or her credit card number for every transaction, a subscriber does not ever have to disclose his or her private key. In the case of fraudulent real estate document filings, digital signatures may greatly reduce the costs associated with forged signatures on real estate documents. It is much easier to forge a signature than to steal a subscriber's private key. Also, smartcards used in conjunction with digital signatures hold the possibility of dramatically reducing the potential for fraud. In France, smartcards

---

51. Biddle, *supra* note 7, at 1242.
52. *See supra* text accompanying note 22.
53. It appears likely that the X.509 standards developed by the International Telecommunication Union will be used for digital signatures. Part 1, Section 4.2 of the X.509 standards is a unique identification field, which might be used to establish who may rely upon a certificate. *See* (visited Feb. 26, 1998) <ftp://ftp.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part1-06.txt> for the latest version of the X.509 standards.
54. *See generally* Froomkin, *supra* note 11, at 76 (discussing the availability and risk of various methods of electronic commerce).

with a password have reduced fraud from about $4 per card in 1992 to almost nothing today.[55] Although smartcards are not generally available at this time in the United States, they have been used in Europe for years, and researchers predict that billions of smartcards will be in circulation by 2000.[56]

Furthermore, the amount of fraud is only relevant when considered in relation to the benefits from the use of digital signatures. If the amount of new business generated by a merchant from digital signatures is ten times the amount of cost he or she incurs from fraud, the merchant will choose to accept digital signatures regardless of the liability scheme imposed. MasterCard and VISA may be losing over $1 billion per year to fraud, but their business is quite profitable. Whether digital signatures will provide enough new business to cover the potential costs from fraud remains to be seen.

There are other reasons why a closed PKI system may not ultimately be the "winner." Such a system inherently requires a contractual relationship between the subscriber, relying party, and certification authority. These contractual obligations introduce extra transaction costs and reduce the efficient use of digital signatures. While this type of arrangement may be adequate for repeated transactions between two businesses, it is not as well suited for consumers or businesses which have only random contacts. Although the certification authority's liability exposure could potentially be solved without a contract through "webwrap" or "click through" contracts, there is presently no case law governing the enforceability of such provisions. Courts are increasingly upholding "shrinkwrap" contracts for software, but those cases involve a clear exchange of consideration. It is less clear whether there is sufficient consideration for a "click through" disclaimer to limit the remedies of a relying party. For example, assume that Alice and Bob enter into a written contract, with ordinary signatures. Under the terms of the contract, Bob may assign his economic rights to a third party. An imposter named Izzy obtains a certificate in the name of Bob from Cheapo Certificate Co. by presenting a poorly forged driver's license. Izzy creates a forged contract between Bob and Izzy which purports to transfer all of Bob's economic rights under the contract to Izzy. Izzy then sends the forged contract to Alice and demands payment. Cheapo Certificate Co. has a "click through" limitation on liability that limits its

---

55. Tom Foremski & Paul Taylor, *Smartcards: A Technology Whose Time Has Come*, FIN. TIMES, Oct. 2, 1996, at 1. Smartcards are not tamperproof, however. *See* David Bank, *Smart Cards are Open to New Attack By Hackers, Say Israeli Researchers*, WALL ST. J., Oct. 21, 1996, at B14.

56. Foremski & Taylor, *supra* note 55, at 1.

liability to a fraction of Alice's potential loss. It seems doubtful that the "click through" limitation would be binding.

Although Biddle believes that a closed PKI system is beginning to emerge as the marketplace winner, such a prediction is premature. Washington's digital signature law does not even become effective until January 1, 1998. Most lawyers are just learning that such a law exists.[57] Other factors will initially slow the growth of an open PKI system. Consumers are not likely to widely use digital signatures until the liability risks are resolved. Also, while the Washington Act establishes clear default rules regarding the use of digital signature in intra-state transactions, the rules for multi-state transactions are less clear. For example, certification authorities licensed under the Washington Act may not have the benefits of statutory limitations on liability if a court determines that the contract between the subscriber and relying party is not governed by Washington law. Because individual state legislation cannot resolve the existing legal uncertainties about digital signatures on a national level, parties will very likely prefer closed system transactions until the federal government enacts national legislation, or a majority of states adopt a uniform digital signature law. While an open PKI system may be slower to develop, that itself is not a reason to reject digital signature laws such as the Washington Act. Digital signature legislation potentially has many benefits. If digital signature laws do not hinder private party transactions and do not force parties to assume liabilities they would otherwise avoid, the reasons for opposing such legislation disappear.

In any event, trying to predict a winner between open and closed PKI systems may not be a worthwhile exercise. The line between an open and closed system will likely become increasingly blurred as more states adopt variations of the Utah Act, but give parties the freedom of contract.[58] Parties will contractually modify the statutory default rules, creating a hybrid system. Ultimately, however, if more states adopt digital signature legislation, the levels of fraud become known, and digital signatures provide real benefits to consumers, parties will increasingly use an open PKI system.

---

57. *See generally*, Rodin, *supra* note 18, at 3 (introducing the subject of digital signatures to the Business Law Section of the Washington State Bar Association).

58. *See Role of Certification Authorities*, *supra* note 35, at 6.

III. CONCLUSION

There are many technological and legal barriers that will slow the growth of electronic commerce. The task confronting legislators and policymakers is to draft legislation to overcome these barriers using the same principles that have guided the development of other commercial laws. As Grant Gilmore observed, legislation should be "designed to clarify the law about business transactions rather than to change the habits of the business community . . . ."[59] The Washington Electronic Authentication Act clarifies the law regarding the use of digital signatures. It will not legislate market winners because it gives parties the freedom of contract. However, the default rules established by the Washington Act should reflect existing business expectations. The Washington Act and other digital signature legislation will not satisfy this principle until limitations on consumer liability are enacted.

59. Grant Gilmore, *On the Difficulties of Codifying Commercial Law*, 57 YALE L.J. 1341 (1948).