

1
2 **TECHNOLOGY NEUTRALITY AND SECURE ELECTRONIC COMMERCE:**
3 **RULE MAKING IN THE AGE OF "EQUIVALENCE"**
4

5 **Michael S. Baum***
6

7 ©1999 VeriSign, Inc.

8 Exposure Draft Version 1.1
9

10 **Abstract:**
11

12 Policymakers are currently confronted with a variety of proposed approaches to
13 promoting secure electronic commerce worldwide. Some of these approaches, each based
14 on certain assumptions concerning the marketplace, technology, and law, include a
15 preference for "technology-neutral" rules, accommodation of various technologies as
16 public key infrastructure (PKI) equivalents or alternatives, and a call for electronic
17 commerce rules that refrain from specifically addressing PKI. This paper examines the
18 advantages and disadvantages of these policy approaches and related legal initiatives on
19 electronic commerce. It argues that PKI is uniquely suited to the needs of secure e-
20 commerce; that PKI's singular capabilities and features have been ignored by those
21 demanding "equivalence" between PKI and other, less-effective technologies; that as a
22 result, the advantages of PKI have not been fully exploited to date; and that PKI-specific
23 rules are needed to provide the necessary certainty to grow the market and ensure global
24 interoperation.

* VP, Practices and External Affairs, VeriSign, Inc. <michael@verisign.com>. *Comments and editorial suggestions are respectfully solicited.*

The author gratefully acknowledges the comments and suggestions from the following reviewers: Joseph Alhedeff, Esq., Prof. Mads Anderson, Dwight Arthur, Juan Andres Avellan, Ken Ayer, Phillip Hallam-Baker, Ph.D., Mark Bohannon, Esq., Jim Brandt, Herald Burman, Esq., Kaye Caldwell, Denley Chew, Esq., Bruce Crabtree, Warwick Ford, Ph.D., Todd Glassy, Ben Golub, Tom Honey, Robert Junneman, Christopher Kuner, Esq., Charles Merrill, Esq., Michael Myers, Ray Nimmer, Esq., Larry O'Gorman, Ph.D., Eric Pearson, Esq., Arem Perez, Rita Proano, Thomas Smedinghoff, Esq., Hon. Renaud Sorieul, Jeff Stapleton, Jim Wayman, Ph.D., Frank Walsh, Esq., Peter Williams, and Steven Wu, Esq.

This paper (or an updated version) is available at
<http://www.verisign.com/repository/pubs/tech_neutral>. Permission is granted to reproduce this paper provided it is done so in its entirety, complete with attribution and this copyright policy.

25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41

TABLE OF CONTENTS

Introduction

Part 1 - The Context of the Debate Over Technology Neutrality

- a. Digital Signatures and PKI**
- b. Biometrics**
- c. Signing Ceremonies**
- d. Debates over Definitions**
- e. The Policy Context**

Part 2 - Open and Closed Systems

Part 3 - Minimalist Laws

Part 4 - Toward a Model PKI Law

- a. Safeguarding Subscriber Private Keys**
- b. Certificate Status Checking by Relying Parties**
- c. Presumptions**

INTRODUCTION

42
43
44
45
46

The world is getting “wired together” at an amazing rate, fueling an explosion in global electronic commerce that shows no signs of slowing. Indeed, analysts foresee a staggering increase in e-commerce in the coming years, predicting as much as \$2 trillion in annual Internet-based commercial transactions by 2002.¹ It is “a question of when, and

¹ The CEO of Cisco, Inc., estimated \$1 trillion to \$2 trillion worth of goods and services will be sold via the Net by 2002. See Edward F. Moltzen, *Cisco CEO Predicts Huge Web Growth*, TECHWEB NEWS, Oct. 13, 1998. Forrester Research, Inc. (<www.forrester.com>), projects global electronic commerce at between \$1.4 and \$3.2 trillion by 2002. See INTERNETWEEK, Nov. 9, 1998, at 7, available at <<http://www.internetweek.com>>. The Organization for Economic Co-operation and Development (OECD) claims that e-commerce may rise to \$1 trillion by 2005. See ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, THE ECONOMIC AND SOCIAL IMPACTS OF ELECTRONIC COMMERCE: PRELIMINARY FINDINGS AND RESEARCH AGENDA, at ch. 3 (1998), available at <http://www.oecd.org/subject/e_commerce/summary.htm>. Others claim that Internet transactions could top \$400 billion by 2002, and no end is in sight. See Jim Hu, *\$400 billion seen in e-commerce*, CNET NEWS, Aug. 17, 1998, available at <<http://www.news.com/News/Item/0,4,25341,00.html>>. The International Data Corporation (IDC) (<www.idcresearch.com>) projects that global Internet-based spending—which includes

47 not if, the Internet will become more crucial than the interstates.”² The comparison is a
48 fitting one: the Internet has the potential to provide a seamless global communications
49 and commerce infrastructure similar to the national transportation and commerce
50 infrastructure provided by the U.S. interstate highways. Moreover, just as there was
51 resistance at first to the idea of building a federally financed and regulated national
52 highway system, so has there been criticism of proposals for enabling a global
53 infrastructure to facilitate worldwide e-commerce. In the 1950s, the debate involved
54 whether government resources should be used to create and support a national
55 transportation system that would favor automobile and truck commerce, even though
56 various alternatives (e.g., rail, boat, or air transport) could be conceived of as well.
57 Today, the argument is whether legal structures should be created to advance specific
58 technologies that support secure e-commerce, even though other such technologies could
59 conceivably be developed in the future

60

61 Specifically, the debate focuses on the extent to which the law should recognize
62 and support the technology of public key infrastructures (PKIs). The term *PKI* is used to
63 refer both to a certification infrastructure based on public key technology and to the
64 discrete components of such an infrastructure, including certification authorities,
65 certificates, digital signatures, and the hardware and software used to implement the
66 infrastructure.³ Partly as a result of the arguments of interest groups averse to this
67 technology, there seems to be a growing tendency among policymakers to follow a
68 “technology-neutral” path concerning e-commerce—that is, to enact policies intended to
69 ensure legal “equivalence” among various technologies for promoting secure e-
70 commerce.⁴

everything from retail sales to business-to-business transactions—will reach \$32.4 billion in 1998, up from \$12.4 billion in 1997. IDC projects that by 2002 annual e-commerce spending will total \$425 billion. The U.S. Department of Commerce offers a more conservative estimate of \$325 billion. *See Internet Commerce and Infrastructure*, THE RED HERRING, Sept. 1998, available at <<http://www.herring.com/mag/issue58/internet.html>>. According to the Gartner Group, by 2003 the Internet will have become the predominant mechanism for conducting business—either with retail consumers or between businesses. *See* John Gartner, *Internet Will Become Core of Business By 2003*, TECHWEB, Oct. 14, 1998, available at <<http://www.techweb.com/wire/story/TWB19981014S0014>>. *See generally*, U.S. DEPARTMENT OF COMMERCE, THE EMERGING DIGITAL ECONOMY (1998), available at <www.doc.gov/ecommerce/EmergingDig.pdf>. *Cf.* Clinton Wilder, *E-Commerce Myths and Realities*, INFORMATIONWEEK, Dec. 7, 1998, 52-63 (debunking “the eight biggest myths about E-commerce,” including its growth, cost, and import), available at <<http://www.informationweek.com>>.

² Steven Levy, *Living with the Bugs*, NEWSWEEK, Aug. 17, 1998, at 68.

³ *See* Michael S. Baum & Warwick Ford, *Public Key Infrastructure Interoperation*, 38 JURIMETRICS J. 359, at 359 n.1 (1998); *see also infra* Part 1 (defining PKI, digital signatures, and certificates).

⁴ For example, consider the following from draft U.C.C. Art. 2B:

71

72 *Technology neutrality* is more a political buzzword than a clearly defined legal
73 concept. In its most common usage, it refers to laws, regulation or other types of rules
74 which purports to favor neither PKIs nor other technologies. The myth advanced by the
75 technology-neutrality lobby is that such rules will ensure the unfettered development of
76 diverse information security technologies and solutions, ensure mutual recognition of e-
77 commerce transactions, and prevent non-tariff trade barriers to global competition for e-
78 commerce services.⁵ But myth is not reality. Those who argue that e-commerce policy
79 must exclude specific legal support for PKI in the name of technology “neutrality” are in
80 fact seeking to preserve a market for various other technologies—technologies that have
81 not yet been invented or demonstrated to be technically sound or practical for the needs
82 of secure e-commerce. Thus the language of “neutrality” is sometimes used to undermine
83 support for an already proven and available technology.

84

The definition is technologically neutral. Statutes in some states give special recognition to “digital signatures” that rely on a specific encryption technology and a certification or licensing system. The procedures established under that type of legislation qualify as an authentication for purposes of Article 2B. The Article 2B concept is broader, however, and recognizes that technology and commercial practice are constantly changing and provide many different ways of achieving an authentication.

Henry Beck, *Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series Drafting, Negotiating and Enforcing Trademark, Copyright and Software Licensing Agreements A Satellite Program*, UNIFORM COMMERCIAL CODE ART. 2B LICENSES, 517 PLI/P 287 (1998).

See draft U.C.C. Art. 2B (Aug. 1, 1998), available at

<<http://www.law.upenn.edu/library/ulc/ulc.htm>>; see also draft U.C.C. § 2B-114 Reporter’s Note 2 (Aug.1, 1998), available at <<http://www.law.uh.edu/ucc2b/080198/080198.html>>.

⁵ A technology-neutral approach *can* be helpful, with certain limitations. It is not the intention of the PKI community to impede the development of alternative technologies; rather, it is our desire to make current technology more available and more useful for real-world applications. This can be done by objectively reviewing what the various available technologies can do, grouping them according to their attributes of security, reliability, scalability, and so on, and creating legislative constructs (including for self-regulation) appropriate to each technology.

85 Some states, including Minnesota,⁶ Utah,⁷ Washington,⁸ and at least a few
86 countries, including Germany,⁹ Italy,¹⁰ Malaysia,¹¹ and Singapore,¹² have enacted
87 comprehensive digital signature legislation with specified requirements and loss
88 allocation rules for a system where security, at least in part, is based upon a *trustworthy*
89 *PKI*. These statutes are sometimes cited as examples of overregulation,¹³ but some of
90 them may very well prove effective at fostering trustworthy PKI systems (although
91 further evaluation of their economic impact is needed). And, of course, nothing would
92 preclude any of these jurisdictions from addressing non-PKI techniques in the future. The
93 great danger, as this paper will demonstrate, lies in allowing the pendulum to swing too

⁶ Minnesota Electronic Authentications Act, MINN. STAT. ANN. ch. 325K (1998), *available at* <http://www.revisor.leg.state.mn.us/stats/325K/>.

⁷ Utah Digital Signature Act, UTAH CODE ANN. §§ 46-3-101 *et seq.* (1998), *available at* <http://www.commerce.state.ut.us/web/commerce/digsig/dsmain.htm>.

⁸ Washington Electronic Authentications Act, WASH. REV. CODE ANN. ch. 19.34 (1998), *available at* <http://www.wa.gov/sec/ea/dsrcw.htm>; *see also* WASH. ADMIN. CODE ch. 434-180 (1998), *available at* <http://www.wa.gov/sec/ea/dswac.htm>.

⁹ German Digital Signature Law (Aug. 1, 1997), *available at* <http://www.iid.de/rahmen/iukdgbt.html>. *See* <http://www.kuner.com> for an English translation and commentary.

¹⁰ Law No. 59 of 15 March 1997, *available at* <http://www.interlex.com/testi/attietet.htm>. *See* [http://www.aipa.it/english/law\[2/index.asp](http://www.aipa.it/english/law[2/index.asp) for an English translation.

¹¹ Malaysia Digital Signature Bill 1997, *available at* <http://www.cert.org.my/digital.html>.

¹² Singapore Electronic Transaction Bill (adopted June 29, 1998), *available at* <http://www.ech.ncb.gov.sg/view/ech/ETBnill.zip>.

¹³ One frequently cited example of a rule that is purportedly an example of overregulation is that section of the Utah Digital Signature Act, UTAH CODE ANN. § 46-3-405 (1998), that declares a certificate to be an acknowledgement of a digital signature:

Unless otherwise provided by law or contract, a certificate issued by a licensed certification authority is an acknowledgment of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgment appear with the digital signature or whether the signer physically appeared before the certification authority when the digital signature was created, if that digital signature is:

- (1) verifiable by that certificate; and
- (2) affixed when that certificate was valid.

Another is the acknowledged document section of the Washington Digital Signature Act, WASH. REV. CODE ANN. § 19.34.340 (1998). *Cf., infra* Part 4.b (presenting the author's proposal concerning presumptions).

94 far toward “technology-neutral” laws, since failing to deal with the infrastructure
95 essential to effective PKI systems could make it impractical to efficiently enforce
96 obligations entered into over the Net.

97

98 Some of the current enthusiasm for technology neutrality comes from a tendency
99 to confuse two related but distinct goals: (1) promoting e-commerce, using the law as a
100 tool; and (2) removing legal barriers to the use of computer-based technologies in
101 commerce. As a result of a more-than-fifteen-year effort to remove such barriers, a large
102 number of states have enacted legislation equating electronic records and images to
103 traditional writings and signatures. Thus the fight to enable the substitution of electronic
104 for paper-based technologies in business transactions—which was an important one—has
105 largely been won in this country. That cause is distinct, however, from the current call for
106 technology neutrality; indeed, the enabling of electronic transactions is frequently
107 obfuscated and exploited in the current debate over technology neutrality.

108

109 The real issue today is the need for clarity in the technology, policy, and legal
110 underpinnings of a secure infrastructure sufficient to facilitate global secure e-commerce.
111 Although other technologies capable of providing such rigor may emerge in the future, at
112 present PKI interoperation¹⁴ best (and sometimes exclusively) satisfies the security
113 requirements seen as critical to Internet-based e-commerce—confidentiality, source
114 authentication, access control, data integrity, and support for nonrepudiation.¹⁵ The secure
115 transfer of information over the Internet requires a concrete, reliable, shared security
116 mechanism or infrastructure; it is not achievable through abstractions and generalities.
117 The real policy issue is whether the law should proactively promote e-commerce or
118 simply leave it to grow or founder on its own, despite the immense economic
119 opportunities the new world of e-commerce offers.¹⁶

120

121 Confusing matters even further, some governments have asserted the prominence
122 of the “closed” PKI commerce model and the eclipse of the “open” PKI model. The
123 difference between “open” and “closed” systems has not been carefully defined, however

¹⁴ See Baum & Ford, *supra* note 3, at 243-60.

¹⁵ See *infra* Part 1 (describing these technology terms and concepts). Note that digital signatures do not inherently allow parties to ascertain who used a particular key, only that someone with access to the key has used it.

¹⁶ As an aside, the debate over technology neutrality cannot be divorced from some of the larger economic and political issues influencing regulatory policy generally. For example, one European stressed that a “way must be found to bring the Frankenstein of deregulated global financial markets under control.” Roger Cohen, *Redrawing the Free Market, Amid a Global Financial Crisis, Calls for Regulation Spread*, N.Y. TIMES, Nov. 1, 1998, at A17 (quoting Jean-Paul Fitoussi, Economic Advisor to the French Prime Minister).

124 (as I discuss in more detail below). The argument concerning which model will
125 eventually dominate electronic commerce can be rationally and factually addressed, but
126 this can effectively occur only after shared understandings of these terms have been
127 achieved. In fact, systems that are more open than closed are growing and are likely to
128 dominate Internet commerce in the future. The position that the contrary is true is mostly
129 polemics, rather than the result of a close analysis of the situation. Nevertheless, this
130 stance has had the unfortunate effect of impeding the development of PKI rules, due to
131 the belief that “closed” systems can rely on private contracts and the principle of party
132 autonomy and thus do not require specific legislation. The focus on open versus closed
133 PKI has also tended to confuse the marketplace.¹⁷ But despite exaggerated reports of its
134 demise, open PKI provides a clear advantage over closed PKI in that it is designed
135 specifically to deliver the interoperability required for Internet-based electronic
136 commerce. So, despite some short-term enabling of purely closed systems, more open
137 systems are the future of secure e-commerce.

138

139 Policymakers, businesses, and consumers must all deal with the realities of our
140 increasingly complex information-based economy. This economy demands greater
141 certainty to compensate for greater threats — requiring more, not less, careful
142 examination of the pertinent security issues. An analogy can be drawn to the electric
143 power and communications industries. Could we imagine failing to consider separately
144 the specific technologies used to generate electricity, such as that generated from nuclear
145 power plants versus that generated from geothermal turbines or windmills? Similarly,
146 could we imagine neglecting to develop laws specifically governing communications
147 satellites (or even the telephone) and relying instead solely on existing generic
148 telecommunications legislation (such as the Communications Act of 1934¹⁸)? The

¹⁷ See *infra* Part 2, Open and Closed Systems; U.S. DEPARTMENT OF COMMERCE, *supra* note 1, at 124 (arguing that “[c]ompetition and consumer choice should be the guiding principles of Internet commerce”).

¹⁸ 47 U.S.C. §§ 151 *et seq.* Indeed, an Internet-related amendment to the Communications Act of 1934 was proposed in 1998 to establish a national policy against federal and state regulation of Internet access and online services, and to maintain Internet commerce free from foreign tariffs and trade barriers. See H.R. 3849, 105th Cong. (1998).

The FCC wields enormous discretion regarding emerging technology. For example, in the early 1980s, it asserted jurisdiction over Internet service providers (ISPs) (which the FCC determined provided “enhanced services”) and then exempted those ISP services from the requirements of telephone regulation. Accordingly, ISPs are not required to pay access charges, file tariffs, or otherwise adhere to “common carrier” rules. An effort to bring Interstate telephony under those common carrier rules (launched by a telephone company industry association) has languished at the FCC for years. Also, Congress dealt with emerging technology (poorly) in the Telecommunications Act of 1996 by specifically directing the FCC, in Section 706, to foster the development, growth, and deployment of advanced technologies. Although the law was enacted

149 inherent complexity of information security, particularly within the context of the
150 Internet, parallels that of electric power and other technologies where policy makers have
151 seen fit to regulate some specific technologies (i.e., nuclear) for the public good, without
152 stifling the development of other promising technologies and markets.

153

154 Thus it is fair to ask if technology neutrality is best for the advancement of secure
155 e-commerce. Indeed, it is fair to ask if it can even work in today's Internet-centered e-
156 commerce environment.¹⁹ Despite the implications of this issue, little has been written on
157 it that transcends anecdotal accounts or political fodder. What is needed is a cogent
158 evaluation of technology-neutral policy and a comprehensive analysis of how much detail
159 is necessary in e-commerce laws to satisfy the complex security, interoperability, and
160 usability requirements of Internet-based e-commerce. This paper aims to bring that
161 objective closer to realization. The paper begins with a review of the technological,
162 historical, and cultural context of the technology-neutrality debate, provides a discussion
163 of open and closed systems, and then moves to a consideration of specific policies and
164 policy issues. It is my hope that, at a minimum, this paper will contribute to a modest
165 derailing of the "technology-neutral" locomotive before the impending train wreck and
166 serve as a basis for further study.

167

PART 1

168

THE CONTEXT OF THE DEBATE OVER TECHNOLOGY NEUTRALITY

169

170 To understand the differences between the various e-commerce policy approaches
171 that different stakeholders have proposed, it is helpful to understand the different
172 technologies and systems that have been developed to enable e-commerce, and to refer to
173 these technologies using clear, shared definitions. This section provides a brief discussion
174 of two such technologies: digital signatures and biometrics. Because of the confusion
175 surrounding the proper use of one particular biometric technique, signature dynamics,
176 and the politics associated with it, this section then turns to a consideration of that
177 technique's specific merits and limitations. It is hoped that this discussion will be of
178 modest assistance to e-commerce rule makers in particular.

179

in February 1996, the FCC is still wrestling with regulation to implement this Congressional mandate.

¹⁹ To date there has been no comprehensive analysis substantiating the oft-heard claim that a technology-neutral approach is the best route for the future development of e-commerce. There is a sore need for the appropriate economic tools to evaluate the regulatory impact of particular types of e-commerce rules.

180 **a. Digital Signatures and PKI**

181 *Digital signatures* are sometimes described as an electronic analog of handwritten
182 signatures. Although they may often be used as a substitute for traditional signatures (or
183 for similar purposes), they have unique functional and legal attributes that are different
184 from those of handwritten signatures. Digital signatures provide assurances of the
185 authenticity of electronic records, as well as other important security services, by
186 transforming the electronic documents or messages with which they are associated. They
187 accomplish this “using an asymmetric cryptosystem and a hash function such that a
188 person having the initial message and the signer’s public key can accurately determine
189 (1) whether the transformation was created using the private key that corresponds to the
190 signer’s public key, and (2) whether the initial message has been altered since the
191 transformation was made.”²⁰ To put this another way, digital signatures utilize a key pair
192 consisting of a key that is kept secret by its holder (the *private key*) and a corresponding
193 key that is (or can be) made public (the *public key*) without compromising the private
194 key. To digitally sign a message, the signer applies his or her private key to it. The digital
195 signature is not the private key itself; rather, it is a number, unique to that particular
196 signed message, that is generated when the private key is applied to the message.
197 Therefore, every digitally signed message contains a unique digital signature. It is
198 computationally infeasible to ascertain a user’s private key by evaluating a digital
199 signature from one of his or her messages.

200

201 The recipient of a digitally signed message may verify the authenticity of the
202 message’s digital signature (and thus of the message itself) by applying the signer’s
203 public key to the message and digital signature. Only the public key that corresponds to
204 the private key used to sign the message will “match,” thereby verifying the authenticity
205 of the digital signature. To do this, the recipient must possess a copy of the signer’s
206 public key. One efficient way for a message recipient to obtain a copy of the signer’s
207 public key is by obtaining the signer’s *digital certificate*. A digital certificate is simply a
208 secured data record that contains the signer’s public key, indicates the “binding” (or
209 association) between that public key and the signer, and is itself digitally signed by the
210 issuer of the certificate – a *certification authority* (CA). As stated above, the term *public*
211 *key infrastructure* (PKI) refers “both to a certification infrastructure based on public and
212 private cryptographic keys and to the discrete components of such an infrastructure,
213 including certification authorities, certificates, digital signatures, and the hardware and
214 software that implements the infrastructure.”²¹

²⁰ INFORMATION SECURITY COMMITTEE, SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE § 1.11 (1996) [hereinafter DIGITAL SIGNATURE GUIDELINES], *available at* <<http://www.abanet.org/scitech/ec/isc/home.html>>. The *Digital Signature Guidelines* also include an excellent tutorial on digital signatures, *see id.* at 3-16.

²¹ Baum & Ford, *supra* note 3, at 359 n.1. *See generally*, JALAL FEGHHI ET AL., DIGITAL

215

216 PKI has two properties that make it particularly well suited to electronic
217 commerce and, in particular, Internet-based commerce. Most importantly, when properly
218 implemented it enables parties to promptly, reliably, and automatically authenticate
219 messages—as well as encrypt and decrypt them— without the need for prior direct
220 sharing of keys between the signer and the recipient. Rather, the parties need only know
221 the public key of the certification authority that issued the certificate containing the
222 user’s public key. This unique property of PKI permits global reliance on digitally signed
223 messages without the logistical nightmare of key distribution by each party.

224

225 Another unique property of PKI that is critical for secure electronic commerce is
226 its support for nonrepudiation. One definition of *nonrepudiation* is “[s]trong and
227 substantial evidence of the identity of the signer of a message and of message integrity,
228 sufficient to prevent the party from successfully denying the origin, submission or
229 delivery of the message and the integrity of its contents.”²² Stated in simpler terms,
230 providing nonrepudiation means the ability to demonstrate that a message was
231 communicated by a particular sender and was not altered in transit, thereby preventing
232 the sender from successfully denying that its origin or contents were sent. The primary
233 issue concerning nonrepudiation is not whether a particular technology can absolutely
234 *guarantee* it but whether the technology directly and materially *supports* it as a function
235 of its inherent design and engineering features.

236

237 For example, a symmetric cipher (a “single-key” cipher that is shared by both the
238 originator and the intended recipient of a message) cannot by itself directly and
239 materially support nonrepudiation. Because either the originator or the recipient can
240 encrypt or decrypt the message (with the same, shared key), there is nothing inherent in
241 the technology of symmetric ciphers that will assist in resolving a dispute concerning
242 who sent a message or what were the contents of the message sent. Using a symmetric
243 cipher, it is true that the recipient can successfully *authenticate* the source and contents of
244 the message, because the recipient knows for certain that there was no forgery or
245 modification by the recipient. But if the sender falsely denies sending the message, the
246 symmetric cipher will be of little use to the recipient in proving *to a neutral third party*
247 that the sender’s denial is false. The third party will be unable to resolve the dispute other
248 than by a speculative weighing of the recipient’s word against that of the sender. In
249 contrast, if asymmetric ciphers (a “dual-key” cipher) using a key pair to create and verify

CERTIFICATES - APPLIED INTERNET SECURITY 61-89 (1998).

²² DIGITAL SIGNATURE GUIDELINES, *supra* note 20, § 1.20. See WARWICK FORD & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE, at ch. 8 (1997) (providing a technical and legal review of nonrepudiation), available at <<http://www.prenhall.com>>. Note that e-commerce professionals are generally aware that the term *nonrepudiation* can have a particular meaning that is somewhat different than the meaning in contract law.

250 digital signatures are used, it is infeasible for the recipient-verifier of a message to forge
251 or modify the message without detection. Accordingly, the neutral third party does not
252 need to trust the word of the recipient that the recipient did not forge or modify the
253 message, and nonrepudiation is supported.

254

255 Support for nonrepudiation within the context of PKI requires assurances that a
256 signer's private key is accessible only to the signer. Such assurances can be enhanced by
257 physically isolating the signer's computer, such as by locking it in a closet (but this is
258 often impractical). Another way to protect a private key is by placing it in a
259 *cryptomodule*, using an access-control technology. Such technologies include smart cards
260 and other devices that require a pass phrase to grant access to the private key. For
261 additional protection, access control can be enhanced by requiring the individual seeking
262 access to submit to the measurement of some physiological or behavioral attribute that is
263 unique to him or her. Such measurements and attributes are known as *biometrics*.

264

265 **b. Biometrics**

266 *Biometric identification* uses certain biological characteristics or behavioral traits
267 of individuals to verify their identity electronically. "In general, biometric identification
268 requires sensors to convert a physical characteristic or behavior . . . into a signal that can
269 be stored, or compared to previously stored signals, using a computer. Consequently, the
270 detailed study of such devices requires the disciplines of human factors, biology,
271 psychology, mathematics, statistics, and electrical and computer engineering."²³ A
272 biometric reader measures physiological indicia and compares them to specified values,
273 but unlike a cipher it is not capable of securing information (including a biometric
274 template or sample) communicated over an unprotected system such as the Internet.

275

276 *Signature dynamics* is one form of biometric technology that involves the capture
277 and measurement of various attributes (such as speed, pressure, and direction) of a
278 holographic (handwritten) signature to verify personal identity.²⁴ (In contrast, *digitized*

²³ National Biometric Test Center (last modified Sept. 23, 1998) (visited Jan. 8, 1998)
<<http://www-engr.sjsu.edu/~graduate/biometrics/index.html>>. Dr. Jim Wayman notes that "DNA
and all other 'forensic' identification techniques, including latent fingerprint identification,
require extensive expert human processing and are not automatic. Therefore, they are not
'biometric identification techniques' according to the definition I use." E-mail from Jim Wayman,
director, National Biometric Test Center, to Michael Baum (Nov. 29, 1998) (on file with author)
[hereinafter Wayman E-mail].

²⁴ As an aside, the California Digital Signature Regulations misleadingly define signature
dynamics as "measuring the way a person writes his or her signature by hand on a flat surface and
binding the measurement to a message *through the use of cryptographic techniques*." CAL. CODE
REGS., tit. 2, § 22003(b)(1)(D) (1998) (emphasis added), *available at*
<<http://www.ss.ca.gov/digsig/regulations.htm>>. Signature dynamics do not necessarily utilize

279 *signatures* are simply electronic facsimiles of holographic signatures, such as those
280 resulting from scanning handwritten signatures into a computer.) Some signature
281 dynamics advocates erroneously claim that it is a viable “alternative technology” to PKI,
282 providing a level of security comparable to that provided by digital signatures, and that it
283 should therefore be afforded the same legal status as digital signatures.²⁵ As I detail later,
284 this claim is not supported in fact.

285
286 Although some biometric techniques do possess unique strengths that make them
287 well-suited to specific narrow applications, by themselves they are insufficient to enable
288 secure e-commerce—the strength and breadth of their security features are simply too
289 limited. PKI offers distinct advantages over biometrics for diverse e-commerce
290 applications, particularly global commerce conducted over the Internet. PKI offers a
291 tested, extensible infrastructure that facilitates commerce conducted over unsecured
292 paths.²⁶ Biometric technologies alone simply cannot provide this (since biometrics is not
293 PKI); however, they can be used to *supplement* that infrastructure (by securing access to
294 a PC, for example) when particularly strong assurances of identity are essential, as
295 discussed later in this paper.²⁷

296

297 Despite biometrics’ drawbacks in terms of facilitating secure e-commerce, the
298 successful uptake of the signature dynamics lobby’s message that their technology
299 represents a viable alternative to PKI has been surprisingly (and unfortunately)
300 remarkable. The success of this message stems in part from the seeming correlation
301 between signature dynamics technologies and ordinary handwritten signatures. For
302 people without technical expertise, the fact that a simple holographic (traditional) signing
303 act is involved may imply that the legal benefits of a *signing ceremony* have been

cryptography per se. *See* sources cited in note 21 above.

²⁵ “Recently it has been suggested that electronic documents authenticated using biometric techniques should be viewed as the legal equivalent of documents authenticated using cryptographic digital signatures. However, equating or conflating these two techniques risks serious confusion as to the respective merits of the two different technologies.” R.R. Jueneman & R.J. Robertson, Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 JURIMETRICS J. 427, 428 (1998). *See infra* table 2 (presenting security services of these technologies).

²⁶ PKI is an *enabling* technology, rather than an end-user application like e-mail, fax, or telex. Also, since e-commerce transactions in most sectors are predominantly business-to-business (and, often, automated and device-to-device rather than human-to-human), depending on biometrics would present an obstacle.

²⁷ “By itself, a biometric solution can enforce a sense of false security. It’s like installing a state-of-the-art home security system with a motion detector and a sensor for each window and door but only on the first floor.” Barry Keyes, *Trust in the Web’s Global Village*, SC MAG., Dec. 1998, at 66.

304 achieved, and the absence of such an act may imply that such benefits have not been
305 achieved. This is not the case, however, as I discuss in more detail below in Part 1.c.
306 Nevertheless, the signature dynamics lobby has stressed the legal effects of signing
307 ceremonies in a strategic effort to establish signature dynamics as a viable substitute for
308 PKI, ignoring the fact that biometric technology does not address computer and network
309 security.²⁸

310

311 There are many other biometric technologies that have not been highlighted in
312 this debate, many possessing security features and cost-effectiveness at least on a par
313 with signature dynamics. Table 1²⁹ identifies leading biometric technologies and
314 describes some of their distinguishing attributes.³⁰

315

²⁸ Moreover, the use and availability of signing ceremonies is an entirely separate issue from the unique attributes of signature dynamics products. Indeed, signing ceremonies are available with diverse other types of e-commerce and information security technologies, including, of course, PKI. A prominent example is the digital signature-based signing ceremony of an Ireland-U.S. joint communiqué on electronic commerce between Bertie Ahern, Prime Minister of Ireland, and President Clinton. *See Communiqué issued by the United States of America and Ireland on Electronic Commerce* (Sept. 1998), available at <http://www.baltimore.ie/clintonvisit98/communique.html>.

²⁹ This table is derived in part from e-mail from Phillip Hallam-Baker, D.Phil, to Michael S. Baum (Sept. 14, 1998) (on file with author). *Disclaimer*: Information in this chart is intended to be broadly representative of the typical performance of commercial products based on the listed techniques. The information is derived from various sources, including vendors' technical specifications and interviews. The comparison of biometric techniques is difficult because of the lack of standardized and objective evaluation methodology and testing.

³⁰ Other biometric identifiers include but are not limited to ear and lip structure, facial thermography, fingertip structure, head acoustics, hand veins, head resonance, keystroke dynamics, knuckle creases, odor, palm print scanning, vein scanning, and wrist veins. *See generally* ACCREDITED STANDARDS COMMITTEE X9, BIOMETRIC INFORMATION MANAGEMENT AND SECURITY WORKING GROUP -- WORKING DRAFT, AMERICAN NATIONAL STANDARD -- X9.84-199X, BIOMETRICS MANAGEMENT AND SECURITY FOR THE FINANCIAL SERVICES INDUSTRY (1998).

TECHNIQUE	TYPICAL CROSSOVER ERROR RATE ³¹	UNIQUENESS ³²	STABILITY ³³	COMMENTS
DNA Sample	-	High	-	Likely to be restricted to forensic use.
Dynamic	1:100 ³⁴	Fair	Fair	Intuitive but potentially

³¹ The accuracy of a biometric technique is determined by its false-positive and false-negative rates. Most biometric techniques have a sensitivity threshold that can be tuned to provide an improvement in one factor at the expense of another. It is possible to construct a device that achieves a zero false-positive rate by always issuing a negative result. The *crossover error rate* is the proportion of errors when the false-positive rate and false-negative rate are equal. All error rates are merely approximate, rounded to the nearest order of magnitude. Nonetheless, *because authoritative benchmark data are unavailable for biometric identifiers generally (with the modest exception of fingerprints), it is difficult not only to compare different biometric techniques but also to compare similar products from different vendors. Further research is recommended to mitigate the current indeterminate nature of crossover error rates.*

Of course, the accuracy of identification technologies can be substantially improved by using multifactor authentication – that is, combining biometrics (which verify *something you are*) with PINs (which verify *something you know*) with smart cards (which verify *something you have*).

A similar term is “equal error rate” (EER). “The term ‘equal error rate’ [crossover error rate] is commonly used, but is meaningless for technologies using highly distinctive measures [such as fingerprint and iris] The false match rate (FMR) can be made arbitrarily small by threshold adjustment, the false non-match rate (FNMR) cannot.” Wayman Email, *supra* note 23.

This paper addresses the perspective of “positive identification” only (*proving I am enrolled*) because of its important commercial context — it does not focus on “negative identification” applications (*proving I am not enrolled*), such as social service and national ID projects.

³² *Uniqueness* is the extent to which a physiological attribute underlying a biometric is unique within the population.

³³ *Stability* is the extent to which a physiological attribute underlying a biometric is constant over time for a given subject. Stability and uniqueness are significant because they represent fundamental limitations on the accuracy of the technique.

³⁴ Dr. Wayman claims that the 1:100 EER could only be supported if enrollment and testing are separated by a short period of time. “Credit card companies have always told me that they have not adopted DSV [dynamic signature verification] because of fears over the ‘template aging’ problem.” Wayman e-mail, *supra* note 23. The template aging problem can be reduced through the implementation of *dynamic template reconstruction*. This method permits the programmatic

Signatures				limited. ³⁵ Inherent template aging problem; strong behavioral component.
Face Recognition	1:100 ³⁶	Poor	Poor	Convenient but limited. There are many cases of similar features. Facial features undergo constant change throughout life, especially during childhood and old age, and due to cosmetic surgery.
Finger Image (pore pattern)	1:100	High	Poor	In early stages of development. Pores are difficult to consistently image.

replacement of existing signature samples using a verified signature (as a partial template replacement – *i.e.*, where there are multiple signature samples in the template) for the baseline’s then-most-deviated signature.

See CAL. GOV’T CODE § 16.5 (1998) (providing that a “signature digest produced by signature dynamics technology is capable of verification if ... the handwriting measurements can allow *an expert handwriting and document examiner* to assess the authenticity of a signature”) (emphasis added), *available at* <<http://www.ss.ca.gov/digsig/code165.htm>>. Since signature dynamics are ultimately dependent upon handwriting experts, the following cases are of interest: *United States v. Rosario*, 118 F.3d 160 (3d Cir. 1997) (asserting that “[h]andwriting analysis is at best an inexact science, and at worst mere speculation itself”), and *Perkey v. Department of Motor Vehicles*, 42 Cal. 3d 185 (1986) (holding that fingerprint technology was the only reliable method, and that other techniques such as handwriting samples could be too easily changed).

Additionally, some signature dynamics vendors have claimed that the touch pads incorporated into computers are generally sufficient to capture signatures for identity verification purposes and that such pads provide a ubiquitous installed base (to counter criticism that the cost of capture devices inherently limits the signature dynamics market). Yet, the intended performance characteristics and use of such pads does not provide the level of trustworthiness and accuracy provided by specially engineered signature dynamic capture devices.

³⁵ The intuitive benefits of signature dynamics also pose potential risks, including that the signatory will not appreciate the inherent differences between signing on paper and signing on a signature capture device (recognizing that the security assurances and attributes of signature dynamics will generally differ, perhaps unexpectedly, among applications, devices and environments).

³⁶ Test results in Dr. Wayman’s laboratory have yielded a 5 percent equal error rate when enrollment and testing were done in the same session. *See* Wayman Email, *supra* note 23.

Finger Image (ridge pattern) ³⁷	1:100	High	Poor	Forensic use may preclude acceptability. Vulnerable to a spoofing/replay attack. ³⁸
Iris Scan	Insufficient data ³⁹ 10% FNMR	High	Good	Noninvasive. Uses a video camera. Eye conditions such as conjunctivitis can invalidate scans.
Retina Scan	1:1,000,000 ⁴⁰	High	Fair	Invasive (laser scanning of

³⁷ See generally Larry O’Gorman, *An Overview of Fingerprint Verification Technologies*, 3 ELSEVIER INFO. TECH. REP. (1998) (providing an authoritative review of fingerprint technologies).

For every biometric there is always at least a small percentage of the population on which the technology cannot work. For example, people who due to congenital defect, injury, or amputation do not possess the body parts being scanned would not be able to use certain scanning technologies. This could raise issues of “cyber-discrimination” concerning public access to electronic malls, government services, etc. See Americans with Disabilities Act of 1990 (ADA), 42 U.S.C. § 12132 (1998) (providing that “no qualified individual with a disability shall, by reason of such disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of a public entity, or be subjected to discrimination by any such entity”). The ADA also amends Title II of the Communications Act of 1934, 47 U.S.C. §§ 201 *et seq.*, extending the reach of the ADA to certain public communications.

It has been suggested that *everyone can have a public key, but not everyone can have a practical biometric* — for example, although amputees generally don’t lose all of their fingers or both of their hands, humans have only one set of vocal cords (necessary for voice verification).

³⁸ A *spoofing attack* is an attempt to create bogus authentication credentials. A *replay attack* is a specific type of spoofing attack in which credentials generated by a previous authentication process are replayed. Some attacks can be mitigated by using multiple frequencies of light, one of which is in the near infrared, to examine unique subcutaneous capillary patterns or blood chemistry.

³⁹ The 1996 Sandia test of iris scanning reported a false non-match rate of about 10 percent. F. Boucher et al., *Laboratory Evaluation of the IrisScan Prototype Biometric Identifier*, Sandia National Laboratory, Report No. SAND96-1033 (Apr. 1996). Tests at 3M and BIOTEST also support this finding. BIOTEST is a European Commission ESPRIT-funded project aimed at developing standard metrics for comparing biometric devices. See National Physical Laboratory, *BIOTEST-Project Summary* (visited Dec. 8, 1998) <<http://www.npl.co.uk/npl/sections/this/biotest/summary.html>>.

⁴⁰ According to Dr. Wayman, “[t]he only big retinal scan study was done in 1990 by the

				retina); may cause injuries. Costly, requires sophisticated equipment. ⁴¹
Voice Verification	1%	Fair	Fair	Convenient, but vulnerable to a replay attack, and effectiveness diminished by background noise. ⁴²

316

317

TABLE 1 - BIOMETRIC METHODS COMPARED

318

319

320

There are many fundamental problems and limitations related to the use of such technologies. Some of them were treated in the recent Public Key Infrastructure Symposium sponsored by the *Jurimetrics Journal*:

321

322

323

324

325

326

327

328

329

330

331

Unfortunately, to date no comparable [to digital signatures] objective, agreed-upon measures have been devised for biometric identification devices proposed for use in electronic commerce. Although the use of biometric devices could still qualify as a “secure electronic signature” if agreed to by the parties, there is less certainty as to how these devices could be determined to be “commercially reasonable” or implemented in a “trustworthy manner,” in large part because few if any of the biometric approaches that have been proposed have been fully disclosed to the technical community much less received the technical and scientific community’s endorsement through recognized standards.⁴³

California Department of Motor Vehicles and the Orkand Corporation under contract to the Federal Highway Administration. This study did not use our current methodologies, so results are hard to interpret. The false non-match rate was around 25%.” Wayman Email, *supra* note 23.

⁴¹ A particular retinal scanner could be the subject of a spoofing attack using a fake eyeball.

⁴² In theory, a voice recognition system can be protected against a replay attack by requiring the subject to read a randomly generated phrase. This requires additional software and hardware and assumes that it will remain infeasible to generate a response to a randomly generated phrase using a voice synthesizer. Secure implementation of such a protocol requires that the system be able to distinguish at least among different speakers using enrolled text.

⁴³ Jueneman & Robertson, *supra* note 25, at 427-46. Jueneman and Robertson also note that “even the best biometric identification techniques, used alone, have potential security flaws that can best be overcome by using the digital signature to bind the biometric identifier to the electronic document in question.” *Id.* at 457.

“Only digital signatures, using current technology, provide the combination of authentication, message integrity, and nonrepudiation which is viewed as a desirable complement to the security

332

333 Despite the limitations of biometrics and alternative technologies⁴⁴ for general e-
334 commerce applications, some signature dynamics advocates have created uncertainty and
335 then capitalized on it. Among other things, they have admonished PKI for “unnecessary
336 complexity,” despite the cumbersome logistical requirements of their own technology.⁴⁵
337 The issue was confused by some vendors who were claiming to sell signature dynamics
338 technology when they were actually selling hybrid proprietary products that included a
339 symmetric cipher. Thus, the attempt to have the public engage in a valid comparison of
340 signature dynamics and digital signatures has been a nonstarter. The real tragedy is that
341 the debate has obscured fundamental issues surrounding Internet-based commerce and
342 has unnecessarily handicapped the possibilities for synergism between biometrics and
343 PKI.

344

345 **Satisfying Fundamentals of Secure Electronic Commerce**

346 In considering the proper role of PKI and biometrics in facilitating global e-
347 commerce, we must acknowledge certain fundamentals of secure electronic commerce.
348 These points are so essential to the nature and goals of secure e-commerce that I have
349 dubbed them “commandments for secure electronic commerce.” These commandments
350 are offered here in Box 1.

standards required by the law Other forms of electronic signature were considered, *such as biometric* and digitized signatures [and rejected].” Security and Electronic Signature Standards, 63 Fed. Reg. 43241, 43260 (Aug. 12, 1998) (emphasis added) (proposing regulation implementing the Health Insurance Portability and Accountability Act of 1996, PL 104-191, 110 STAT. 1936 (Aug. 21, 1996)). Also, “[b]iometrics shall not be used as a single factor authenticator within the financial services industries.” ANSI X9.49, SECURE REMOTE ACCESS TO FINANCIAL SERVICES (1998).

⁴⁴ *But see* David Whitaker, VP, Star Bank Corp., 3 Elec. Com. & L. Rep. (BNA) 1163 (Sept. 30, 1998) (claiming that digital signatures are not well-suited for face-to-face transactions). Bank customers who appear before a bank teller, grocery store checkout clerk, or retail vendor increasingly are required to run a debit card through a reader and then input a PIN in order to effect payment. Similarly, smart cards are well suited (and indeed increasingly are used) to hold and secure a customer’s private key. By contrast, some biometric identifiers require too much data for ubiquitous deployment on current chip cards.

⁴⁵ For example, materials from one signature dynamics vendor state that its dynamic signatures “should not be confused with a so-called ‘digital signature,’ which is a complex process involving public key cryptography.” However, signature dynamics requires data processing, additional hardware and software, and, of course, keeping information in non-human-readable form, which makes it anything but simple.

351

352

353

354

I. Only cryptographic methods can provide adequate security for information communicated over open systems such as the Internet.

355

356

357

358

359

II. With few exceptions,⁴⁶ only asymmetric cryptography, such as that invoked by digital signatures, can provide strong support for “nonrepudiation”⁴⁷ for secure *Internet* commerce. Biometric technologies cannot by themselves substitute for cryptographic methods in securing open systems, including the Internet.⁴⁸

360

361

362

III. Biometric techniques can *contribute to system security*, by providing local access control to computer resources, including cryptographic keys.⁴⁹

363

BOX 1 - COMMANDMENTS FOR SECURE ELECTRONIC COMMERCE

364

365

366

367

368

369

These commandments highlight a critical point – there is simply no practical, commercially available technology other than cryptography that can secure information over insecure paths such as those used by the Internet. Approximately twenty-five years have passed since the invention of public key cryptography, and nothing can yet compete with it, including biometrics. Simply stated,

⁴⁶ Some purported exceptions include:

- *One-time pad*. See James J. Mitchell, *Net Security Takes Key Step*, SAN JOSE MERCURY NEWS, Sept. 13, 1998, available at <<http://www.mercurycenter.com/business/top/023026.htm>> (describing how Atalla rejected PKI and took the approach that uses randomly generated numbers that are never replicated in the exact sequence); and

- *Chaffing and winnowing*. See Ronald L. Rivest, *Chaffing and Winnowing: Confidentiality without Encryption* (last modified Apr. 24, 1998) <<http://theory.lcs.mit.edu/~rivest/chaffing.txt>> (describing a technique that “can provide excellent confidentiality of message contents without involving encryption or steganography”).

⁴⁷ See text *supra* at note 22; see also FORD & BAUM, *supra* note 22, at 315-55 (providing an overview of *nonrepudiation*).

⁴⁸ A major problem that can be solved only through the use of asymmetric cryptography is that of key distribution.

⁴⁹ Arguably an additional commandment could be added to the following table: “IV. The selection of cryptographic schemes should be based on their suitability to countering the risks associated with the applications and functions being served, assuming their costs do not outweigh their benefits.”

370

371 [b]iometrics are powerful and useful, but they are not [cryptographic]
372 keys. They are useful in situations where there is a trusted path from the
373 reader to the verifier [or when encrypted information is sent over non-
374 trusted paths]; in those cases all you need is a unique identifier. They are
375 not useful when you need the characteristics of a key: secrecy,
376 randomness, the ability to update or destroy. Biometrics are unique
377 identifiers, but they are not secrets.⁵⁰

378

379 Biometric data (including from signature dynamics technologies) communicated
380 over the Internet can be spoofed (such as by substitution) when not in encrypted form and
381 are comparatively subject to repudiation in the absence of digital signatures.⁵¹ The PKI
382 industry and most recognized cryptographers and security experts understand this and
383 have long emphatically embraced the use of biometrics to *enhance* PKI security, rather
384 than to substitute for it. Again, biometrics are valuable for controlling local access to
385 computer resources and cryptographic keys contained within a cryptomodule⁵²;
386 authorized users can then safely enable digitally signed or encrypted communications
387 over insecure networks or channels, such as the Internet.⁵³ Figure 1 illustrates how
388 biometrics can be used to enhance PKI.

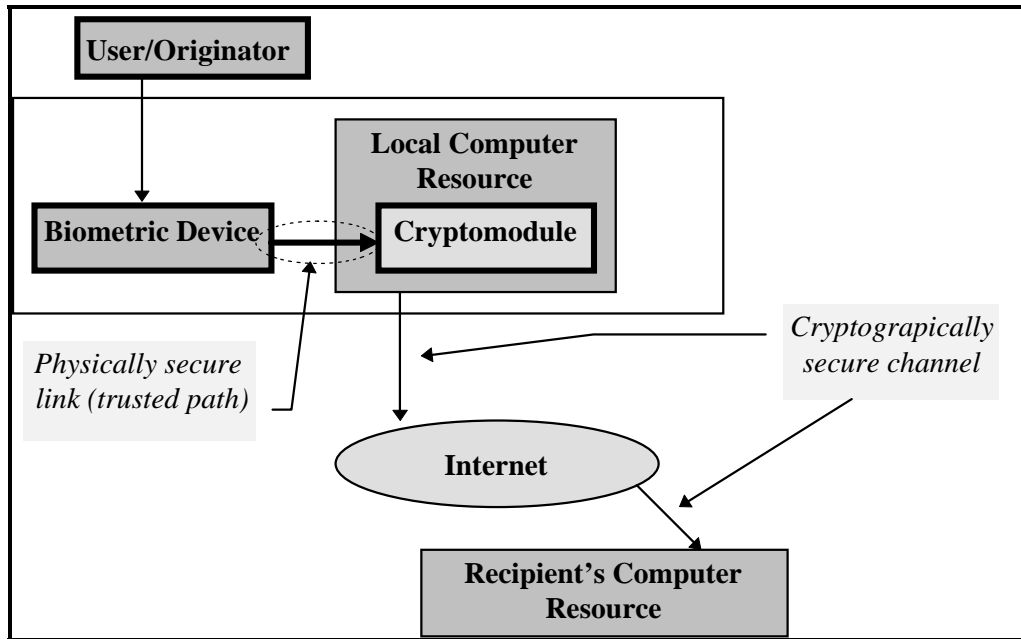
389

⁵⁰ Bruce Schneier, *Biometrics: Truths and Fictions*, CRYPTO-GRAM, Aug. 15, 1998, available at <<http://www.counterpane.com/crypto-gram-9808.html>>. Secrecy is needed to avoid duplication.

⁵¹ “Biometric authentication technologies have limitations when employed in network contexts because the compromise of the digital version of someone's biometric data could allow an attacker to impersonate a legitimate user over the network.” FRED B. SCHNEIDER, ED., COMMITTEE ON INFORMATION SYSTEMS TRUSTWORTHINESS, COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, COMMISSION ON PHYSICAL SCIENCES, MATHEMATICS, AND APPLICATIONS, NATIONAL RESEARCH COUNCIL, TRUST IN CYBERSPACE, at ch. 4 (1998) [hereinafter TRUST IN CYBERSPACE], available at <<http://jya.com/tic.htm>>.

⁵² See NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES (1994), available at <<http://www.itl.nist.gov/div897/pubs/fip140-1.htm>>.

⁵³ For simplicity, Figure 1 does not include a biometric device associated with the recipient's computer for access control and protection of the recipient's private key (here, for message decryption purposes).



390
391

392 **FIGURE 1 - BIOMETRICS AND TRUSTED PATHS**

393

394 The limitations of biometric methods include privacy problems,⁵⁴ spoofing and
395 replay attacks,⁵⁵ the trusted terminal problem (discussed further below), and the

⁵⁴ The use of biometric techniques requires considerable attention to privacy issues. *See generally* Corien Prins, *Biometric Technology Law*, 14 COMP. LAW & SECURITY REP. 159 (May-June 1998) (considering, in part, the implications of biometric data repositories potentially violating the E.U. Directive 95/46 on the Protection of Individuals in Relation to Personal Data, O.J. 1995 L 281/31).

Note that if a central biometric data repository is compromised, then potentially *all* unrelated applications that make use of that data are also compromised. There are a growing number of groups that are resisting the use of biometrics for various reasons. There are also many legislative responses. For example, one California bill states that because the “widespread availability and unauthorized access to [personal] identifiers have led and will lead to a substantial increase in identity-theft related crimes,” it “is the intent of the Legislature to protect the privacy of Californians and the security of personal identifiers by prohibiting unauthorized access to and dissemination of biometric identifiers.” California Senate Bill No. SB 71 (introduced by Sen. Murray Dec. 7, 1998). Perhaps the longer-term regulation of biometrics will put biometric technologies at a competitive disadvantage vis-a-vis PKI.

⁵⁵ *See supra* note 38.

396 nonrepudiation and binding problems.⁵⁶ In addition, there remain serious limitations in
397 our ability to objectively evaluate diverse biometric methods and assess and ensure their
398 equivalency.

399

400 As a summary, Table 2 demonstrates the security services available from the
401 indicated technologies.⁵⁷

402

	BIOMETRICS	DIGITAL SIGNATURES	ENCRYPTION	BIOMETRICS WITH DIGITAL SIGNATURES	BIOMETRICS WITH ENCRYPTION
REMOTE ACCESS CONTROL	No	Yes	No	Yes	Yes
ORIGIN AUTHENTICATION	No	Yes	Yes	Yes	Yes
DATA INTEGRITY	No	Yes	Typically	Yes	Typically
SUPPORT FOR NONREPUDIATION ⁵⁸	No	Yes	No	Yes	No
CONFIDENTIALITY	No	No	Yes	No	Yes

403

⁵⁶ When a document is signed using a handwritten signature or seal, there is typically good (but not irrefutable) circumstantial evidence that the document in question was indeed signed by the person concerned. Relying on biometric technologies to verify a signing may present the same problem with regard to binding, however, that is presented by a signature on a facsimile. Although a signature on a faxed document itself may be irrefutably that of the purported signatory, this does not resolve the question of *which particular document* was signed, since there is no necessary causal binding between the signature and a specific document. (In other words, someone could have affixed the image of the signature, taken from any document, to the faxed document and then transmitted it.) As a result, the applicability of biometric techniques is limited to identification purposes; only digital signatures can provide strong support for binding between specific users and electronic records communicated over the Internet.

⁵⁷ Table 2 is limited to Internet-based commerce applications where there is *no* trusted path, and it assumes that the biometric device is neither logically nor physically secured to the computer resource or cryptomodule in a trusted fashion.

⁵⁸ See text *supra* at note 22 (defining *nonrepudiation*). When a biometric supplements PKI in many applications, the evidentiary value of the signed data may be materially stronger (but, of course, not absolute). This row (in Table 3) reflects this fact and is therefore labeled “*support for nonrepudiation*” rather than simply “nonrepudiation.”

404

TABLE 2 - ATTRIBUTES OF SECURITY TECHNOLOGIES FOR THE INTERNET

405

406

The “Trusted Terminal” Problem

407

408

409

410

411

412

413

414

415

416

417

418

419

“Message Replay” Attacks

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

c. Signing Ceremonies

440

441

442

The term *signing ceremony* has increasingly been used within the e-commerce legal community to denote the act of manifesting parties’ assent to a computer-based

443 contract.⁵⁹ As discussed previously, some have argued that such ceremonies may be less
444 effective, if not totally ineffective, if signature dynamics technologies are not included. In
445 reality, signing ceremonies using technologies other than signature dynamics can produce
446 comparable, if not superior, legally effective results.⁶⁰

447

448 The underlying legal goal of a signing ceremony is to demonstrate the signatory's
449 assent to the intended legal act and to prevent the successful repudiation of that assent. In
450 this regard, signing ceremonies should make clear what is being signed, provide notice
451 and disclosure concerning the proper use of the technologies applied during the
452 ceremony, provide assurance that the signatory's act is purposeful, affirmative, and
453 understood by the signatory, and provide an opportunity to confirm the results of the
454 ceremony. The remainder of this section briefly examines each of these elements.

455

456 i. *Clarity* as to what is being signed

457 A paper document presents its information identically to all
458 readers, whereas an electronic document is malleable, capable of
459 presentation in different styles. The issue of precisely which computer-
460 based records are being signed is independent of any particular signing
461 technology.⁶¹ File attachments and linked Web pages are two examples of
462 data forms that can create confusion concerning record or document
463 "boundaries." Technologies are available to clarify what is being signed
464 independent of any particular biometric or authentication mechanism.⁶²

⁵⁹ For example, draft U.C.C. § 2B-111 (Manifesting Assent) (which is far from being finalized) provides that a person "manifests assent to a record or term of a record if the person acting with knowledge of, or after having an opportunity to review the record or term . . . (1) authenticates the record or term; [or] (2) in the case of conduct or statements of a person, the person intends to engage in the conduct or make a statement and know or has reason to know that the other party may infer from the conduct or statement that the person assents to the record or term" and that "[c]onduct or operations manifesting assent may be proved in any manner." Draft U.C.C. § 2B-111 (Aug. 1, 1998), *available at* <<http://www.law.uh.edu/ucc2b/080198/080198.html>>.

A different approach can be seen in Section 2-206(1)(a) of the U.C.C.: Acceptance of an offer can be made "in any manner and by any medium reasonable under the circumstances."

⁶⁰ *See supra* table 1 (listing diverse biometric technologies).

⁶¹ For example, technologies such as SGML and XML may express abstract structure of a document without deliberately separating presentation issues to be addressed in complementary mechanisms (e.g., style sheets).

⁶² For example, technologies to represent signable documents such as Extensible Forms Description Language (XFDL), a proposed Universal Forms Description Language (UFDL) and

465

466

467

- ii. *Notice and disclosure* concerning the proper use of a ceremonial signing technology

468

469

470

471

472

473

474

Notice and disclosure are largely functions of displaying information in a way that is meaningful to the signatory, independent of the particular signing mechanism itself. For example, a notice could be presented in large flashing type, against a contrasting background, within a triangular “warning” icon, together with an audible “siren.” Or the signatory could be required to scroll through the text of a notice (or, indeed, the complete contract) before being permitted to sign.⁶³

475

476

- iii. *Purposeful and affirmative act* of the signatory

477

478

479

480

481

There are certainly many acts beyond providing one’s handwritten signature that can demonstrate seriousness and purposefulness. One of the most recognized of such acts may be the provision of one’s fingerprint. Generally this is considered an act of greater gravity than simply providing one’s signature. People are certainly less likely to

electronic document approval technologies. *See, e.g.*, ApproveIt (visited Jan. 11, 1999) <<http://www.silanis.com>>. Additionally, leading commercial Web browsers offer public-key related Application Programming Interfaces (APIs) that today enable deployment of these mechanisms." *See, e.g.*, Netscape, *Security Developer Central* (visited Jan. 14, 1999) <<http://developer.netscape.com/tech/security/index.html>> (noting that the capability is "for demonstration purposes only").

⁶³ *See generally* Interpretation of Rules and Guides for Electronic Media; Request for Comment, 63 Fed. Reg. 24996, 25001-04 (May 6, 1998) [hereinafter FTC Interpretation] (considering the application of the FTC’s rules and guides to electronic media, including “clear and conspicuous disclosures in electronic media”); *cf.* Electronic Fund Transfers; Final Rule, 63 Fed. Reg. 14530 (Mar. 25, 1998) (articulating the less onerous standard of “clear and readily understandable”).

In the securities arena, the Securities and Exchange Commission has been required to address the electronic notice issue in the context of trade confirmations. In 1995, the Commission stated that “[u]nder current interpretations of Rule 10b-10, confirmations may not be delivered electronically unless the Commission has specifically permitted such delivery. The Commission has recognized the use of a facsimile machine to send customer confirmations. . . . The Commission . . . also has allowed, under specified conditions, confirmations to be sent by electronic means.” Use of Electronic Media for Delivery Purposes; Final Rule and Proposed Rule Electronic Filings of Forms 3, 4, 5, and 144; Notice, 60 Fed. Reg. 53457, 53459 (Oct. 13, 1995); Thomson Financial Services, Inc., SEC No-Action Letter, [Current Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 76,823 (Oct. 8, 1993) (deeming electronic confirmations as satisfying broker-dealer’s duty to deliver written confirmations to clients).

See also infra note 140 and accompanying text.

482 indiscriminately provide their fingerprint than they are to provide their
483 signature, and in some jurisdictions the law reflects this inclination. (For
484 example, a signatory’s fingerprint is required by notaries in California
485 only in connection with real estate transactions.⁶⁴)

486

487 Independent of the particular signing technology employed, mechanisms
488 can be included to enforce specific (or multiple) actions by the signatory
489 (e.g., requiring a response to a notice that asks, “Are you sure you want to
490 execute this contract?” or requiring the signatory to type, “I agree to the
491 terms of the xyz contract”). For increased certainty as to the meaning of
492 the signing act, a reason code could be required. The use of reason codes
493 was standardized nearly a decade ago for electronic data interchange
494 (EDI)–based signatures to provide this certainty. In addition, the collective
495 set of notices, affirmations, and other corroborating indicia of a legally
496 effective signing ceremony can be archived independent of the particular
497 technology used in such a ceremony.

498

499 iv. *Opportunity to confirm* the results of the signing ceremony.

500 Upon the completion of a signing ceremony, the opportunity to
501 review the documents, verify the signature(s), and affirm the sufficiency
502 and correctness of the ceremonial acts prior to finishing the ceremony is
503 certainly available, and independent of any particular (biometric or other)
504 signing technology used in the ceremony. For example, one could be
505 required to insert a smart card in response to a notice that states,
506 “Important: If you insert your smart card now, you will be confirming that
507 you have signed the xyz document!” as a confirmation technique. The on-
508 line contract and associated content could also be preserved by the
509 signatory.⁶⁵ One benefit of PKI is that the signer may choose (or be
510 required) to verify the integrity of the signing process (i.e., apply his/her
511 public key to verify the digital signature) prior to completing the
512 transaction.

513

514 **d. Debates over Definitions**

515 The technology-neutrality movement has made definitions a battlefield. Perhaps
516 most unsettling has been the attempt to redefine or eliminate much of the recognized,
517 fundamental vocabulary of PKI. Such assaults on accepted definitions, especially in light

⁶⁴ See CAL. GOV’T CODE § 8206(a)(2)(G) (1998).

⁶⁵ See FTC Interpretation, *supra* note 63, at 25000 (proposing a policy that would permit “consumers using electronic media [to] read the information and preserve it for possible later review either by printing it on paper, saving it on disk, or by some other means”).

518 of the technical and legal communities’ often tenuous, but increasingly successful,
519 agreement on shared PKI definitions,⁶⁶ can only create confusion and uncertainty. For
520 example, some technology-neutrality advocates have sought to make the terms *digital*
521 *signature* and *electronic signature* synonymous.⁶⁷ The California Digital Signature Act
522 defines a digital signature as “an electronic identifier, created by computer, intended by
523 the party using it to have the same force and effect as the use of a manual signature.”⁶⁸
524 The interchangeable use of the terms *digital* and *electronic* is incorrect and confusing
525 because of the unique and important security services provided by digital signatures and
526 the otherwise widely accepted meaning of the term *digital signature* (whereas the term
527 *electronic signature* could include almost anything). Also, digital signatures should not
528 be *exclusively* tied to providing the equivalent of paper-based signatures, because digital
529 signatures can serve other functions, such as to ensure integrity without implying any
530 particular legal signing act. Other examples are the proposals to eliminate the term
531 *certification authority* and substitute the term *information certifier* and to eliminate the
532 term *relying party*, purportedly to make the model rules “technology neutral.”⁶⁹

⁶⁶ For example, the American Bar Association’s Information Security Committee recognized the importance of definitions and worked closely with the technical community to advance an appropriate balance of legal and technical requirements in its *Digital Signature Guidelines*, cited above in note 18. Most legislation in the field has adopted or been influenced by its approach and definitions.

⁶⁷ *Electronic signature* is generally recognized to mean “data in electronic form in, affixed to, or logically associated with, a data message, and [that may be] used to [identify the signature holder in relation to the data message and indicate the signature holder’s approval of the information contained in the data message]. See UNCITRAL, draft ARTICLES ON ELECTRONIC SIGNATURES (Dec. 15, 1998), U.N. Doc. A/CN.9/WG.IV/WP.80 [hereinafter UNCITRAL Draft ARTICLES], available at <http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-80.htm>.

⁶⁸ CAL GOV’T CODE § 16.5 (1998). Compare with the definition found in Section 1.11 of the *Digital Signature Guidelines*, cited above in note 18.

⁶⁹ Elimination of the term *certification authority* was proposed in the UNCITRAL Draft ARTICLES “to make it clear that the draft Uniform Rules should also apply to signature technologies which may not be specifically digital signatures, but which may nevertheless utilize similar functions to those characteristic of digital signatures.” UNCITRAL draft ARTICLES, *supra* note 67, Art. A Remark 10. This will likely create confusion between certification authorities, notaries, registration authorities, and other “information certifiers.”

Eliminating the term *relying party* was proposed by the U.S. delegation during the July 1998 session of the UNCITRAL Working Party on Electronic Commerce. Elimination of the terms *key* or *private key* (and the substitution of *device*) were proposed during the Expert group meeting on Digital Signatures held on November 4, 1998.

533 **e. The Policy Context**

534 The movement for technology-neutral rules was initially inspired by the General
535 Accounting Office and the U.S. Comptroller General (which probably did not foresee the
536 attendant policy and implementation complications) in 1991.⁷⁰ It was then catalyzed by
537 the signature dynamics industry and has been the driving force behind some recent e-
538 commerce legislation and regulations. For example, (what I characterize as) the “standard
539 rule” suggested by the U.S. Comptroller General decision was widely implemented (with
540 various modifications), both domestically and abroad, following the birth of the
541 technology-neutrality movement. Although the standard rule ostensibly does not promote
542 any particular technology, it is in fact biased in favor of certain technologies. It
543 establishes the requirements for secure or enhanced electronic signatures and generally
544 permits the use of any authentication technology that ensures that a signature affixed to a
545 data message

546

547 (i) is unique to the signer [for the purpose for][within the context in] which it is
548 used;

549 (ii) can be used to identify objectively the signer of the data message;

550 (iii) was created and affixed to the data message by the signature holder or using
551 a means under the sole control of the signature holder.⁷¹

552

⁷⁰ See U.S. Comptroller General, Matter of National Institute of Standards and Technology—Use of Electronic Data Interchange Technology to Create Valid Obligations, Decision [V]B-245714 (Dec. 13, 1991).

⁷¹ UNCITRAL Draft ARTICLES, *supra* note 67, Art. A, § (b). Compare the following iteration adopted in Section 10-11-(b)(2) of the Illinois Electronic Commerce Security Act:

(A) is unique to the signer within the context in which it is used;

(B) can be used to objectively identify the person signing the electronic record;

(C) was reliably created by such identified person (e.g., because some aspect of the procedure involves the use of a signature device or other means or method that is under the sole control of such person), and that cannot be readily duplicated or compromised; and

(D) is created, and is linked to the electronic record to which it relates, in a manner such that if the record or the signature is intentionally or unintentionally changed after signing the electronic signature is invalidated.

Cf. also CAL. GOV'T CODE § 16.5(a). *But cf.* Draft UNIFORM ELECTRONIC TRANSACTIONS ACT (Sept. 18, 1998) [hereinafter UETA], *available at* <<http://www.law.upenn.edu/library/ulc/uecicta/eta1098.htm>> (rejecting this approach).

553 As described below, the standard rule either favors certain technologies in subtle
554 yet very important ways or sets requirements that are patently inadequate for most
555 Internet commerce applications, thereby allowing inappropriate technologies over the
556 bar. As a policy it fails to exploit security technologies that can leverage the value added
557 by the Internet and is thus either a barrier to *viable* secure e-commerce or has the effect
558 of inappropriately accommodating technologies that are ill-suited to the lion's share of e-
559 commerce applications.

560

561 ***The Need for Prompt or Immediate Verification***

562 Signature dynamics arguably meets the standard rule's requirement that a
563 signature enable the objective identification of the signer. Yet, is this enough? The
564 standard rule stipulates *how* an electronic signature must be capable of being used, but it
565 says nothing about *when* it must be so capable. Much of today's Web-based commerce
566 consists of transactions processed in near real time. Many consumers who connect to a
567 commercial Web site need to know *immediately* whether or not the site is authentic. If the
568 consumer wants to make an on-line purchase (of software or information, for example),
569 he or she expects immediate on-line order processing and delivery.⁷² For example, "Time

⁷² Verification operations by PKI end-users can be performed locally without material performance degradation, and to the extent that on-line certificate status is requested, the marginal cost of a status check is *de minimis*; the necessary infrastructure is available and largely deployed; no technology claims 100% availability (i.e., "all the time"), and yet PKI can perform verification services with more than 99% availability whereas some hybrid biometric-based technologies (such as certain proprietary signature dynamics products) are simply incapable of *any* "prompt and automatic" verification within an Internet commerce environment; and to the extent that "infrastructure" is needed to "perform," such an infrastructure is being widely deployed.

For most Internet commerce, there is compelling reason not to promote the deployment of manual systems for signature verification purposes. Nonetheless, to the extent that any manual processes are appropriate and feasible in such an environment, one must distinguish between (a) the initial one-time *validation* of a certificate applicant's credentials in order to obtain a digital certificate (possibly a manual process) and, (b) the subsequent *verification* of a digital signature (an automated process).

On the other hand, another commentator remarked, "As an example, your handwritten signature on a check is what, in principle, authorizes that funds move from A to B. In truth, from a bank's point of view, actually verifying handwritten signatures is a transaction cost that is not worth bearing unless the cost of verification is less than the risk of loss. At the largest banks, the threshold dollar amount below which verification does not really happen is a closely guarded number, but it generally exceeds \$20,000 and still they have platoons of people doing this all day, every day. Converting the means of signature verification from a manual process into a machine-

570 Warner Inc. changed the way it offered a free trial subscription to a children's magazine
571 from consenting online to offline. The rate of requests for trial subscriptions dropped by
572 95 percent. It kills business. . . [y]ou lose the good side of the Internet."⁷³ Similarly,
573 when a customer presents a credit card to a shopkeeper, all parties (the customer, the
574 shopkeeper, and the parties' respective banks) demand and benefit from the near-
575 instantaneous telephone verification of the customer's credit card status. Thus an
576 increasingly fundamental requirement for most e-commerce is to provide for at least
577 prompt, if not immediate, reliable verification (or other material information).

578

579 PKI permits the verification of messages from unknown parties⁷⁴ in near real time,
580 with great accuracy, at little or marginal cost, and without the need for, *a priori*, special
581 hardware. This capability permits the economical verification of *all* transactions as a
582 matter of course, as standard business practice. This provides many benefits, both
583 tangible and intangible, including greater business certainty, a reduction in losses from
584 fraud, and reduced general and administrative costs, including for insurance.⁷⁵ It also
585 allows managers to develop new or enhanced products swiftly and strategically and to
586 scale the product delivery infrastructure as needed. In contrast, imagine a technology
587 that is legislated to be a PKI "equivalent" or "alternative" that cannot verify transactions
588 from unknown persons on the Internet⁷⁶ and that, in fact, may actually require a
589 handwriting or document expert to analyze and authenticate a signature!⁷⁷ The standard

able one would radically change the economics of check processing. It would add billions to lines and do it from the cost-avoidance side of the ledger." Dan Geer, Sr. Strategist, CertCo, presentation to the Digital Commerce Society of Boston (Nov. 3, 1998) (on file with author).

⁷³ Arthur B. Sackler, VP of Law and Public Policy, Time Warner, Inc., 3 Elec. Comm. L. Rep. (BNA) 1145, at 1155 (Sept. 30, 1998) (testifying on behalf of the Direct Marketing Association before the Communications Subcommittee of the Senate Commerce, Science and Transportation Committee).

⁷⁴ That is, from persons who do not have a pre-existing contractual relationship.

⁷⁵ "If you have poor security, you'll pay higher premiums As data-theft insurance becomes more prominent, you'll see higher levels of security implemented." Beth Davis, *Insurers Plan To Offer Antihacker Policies: Coverage Could Make E-commerce Less Risky*, INFORMATIONWEEK, Oct. 5, 1998 (quoting Jim Balderston, Analyst, Zona Research Inc.), available at <<http://www.informationweek.com/703/03iuins.htm>>.

⁷⁶ Such as PKIs that have their root keys pre-distributed to tens of millions of copies of commercial browsers. See *infra* Part 2 - Open and Closed PKI (describing pre-distributed root keys in greater detail).

⁷⁷ See CAL. GOV'T CODE § 16.5 (providing that a "signature digest produced by signature dynamics technology is capable of verification if: (a) the acceptor of the digitally signed message obtains the handwriting measurements for purposes of comparison, and (b) if signature

590 rule may also discriminate against digital signatures when used only for integrity
591 assurances.⁷⁸

592 ***The Need to Foster U.S. Market Share***

593 The United States currently dominates the PKI industry, but potential foreign
594 competition abounds.⁷⁹ Consequently, the U.S. government should consider PKI rules
595 that facilitate e-commerce and should be particularly supportive of the technologies,
596 architectures, and practices of U.S.-based PKI market leaders, particularly given the
597 potential revenue attributable to PKI relative to its “equivalents” or “alternatives.”
598 Ironically, however, some government offices have privately urged that the U.S.
599 government not support (or at least not facilitate) PKI market leaders. And yet, in the
600 context of considering technology-neutral legislation, some of these same officials claim
601 that the PKI industry is too immature for the government to establish regulations that
602 would facilitate PKI specifically.

603

604 There are few examples of a policy more flawed or damaging to the e-commerce
605 marketplace than efforts to curtail the global availability of strong encryption
606 technologies.⁸⁰ Consider whether the economic impact of proposed technology-neutral

verification is a required component of a transaction with a public entity, the handwriting
measurements can allow *an expert handwriting and document examiner* to assess the authenticity
of a signature” (Emphasis added)); *cf.* Geer, *supra* note 72.

Also, it is ironic to observe the interest and advocacy by factions of the e-commerce legal
community in promoting purely “automated transactions” that do not involve human beings
(clearly a class of transactions for which biometrics have little relevance. *See* UETA, *supra* note
71, § 102(2) (Sept. 18, 1998).

⁷⁸ The standard rule states, “(iv) was created and is linked to the data message to which it relates
in a manner such that any change in the data message or signature would be revealed.” This is
necessarily linked to the earlier part of the rule that states, “(ii) can be used to identify objectively
the signer of the data message.” This is problematic because it restricts the use (or materially
limits the beneficial legal effect) of technology to assure message integrity (exclusive of signature
applications) to enhance the evidentiary status of data. Biometric methods simply do not provide
message integrity security services while cryptographic-based message digests (or “hash
functions”) do. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY (2d ed. 1996); *see also supra*
table 2.

⁷⁹ Examples include Baltimore Technologies (<www.baltimore.ie>) of Ireland, Entrust
Technologies (<www.entrust.com>) of Canada, Signet Assurance (<www.sac.net>) of Australia,
and Xcert International (<www.xcert.com>) of Canada..

⁸⁰ *See, e.g.*, Security and Freedom through Encryption (SAFE) Act, H.R. 695, 105th Cong. (1997)
(containing provisions that would impede global availability of strong cryptography).

607 legislation will parallel the U.S. government's impact on U.S. competitiveness within the
608 encryption industry.⁸¹ Will the frenzy over technology neutrality do to the PKI industry
609 what some claim the government has done to the cryptography industry? The economic
610 impact of these policies on the certification authority industry might be an appropriate
611 area for study by respected academic groups or trade-related intergovernmental

We have already witnessed various legislative proposals that have placed great burdens on the PKI industry. One example is the McCain-Kerry bill, S. 909, 105th Cong. (1997), which would have required certification authorities to provide, at their expense, key escrow capabilities. A statement or analysis of the economic impact of such regulation on the CA industry neither accompanied the bill, nor was it available from any federal agency. Similarly, the application of this Act to the PKI industry and its associated economic burden have not been addressed to date. Compare the Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010 (1998).. Also, a step towards similear legislation was made in late 1998 with the Wassenaar Arrangement. See <<http://www.wassenaar.org>>.

⁸¹ This may be particularly relevant given the reliance of the U.S. certification authority industry on the availability of trustworthy, end-user cryptomodules. Note the revised Administration's encryption policy, see Press Release of Bureau of Export Administration, U.S. Department of Commerce, Dec. 30, 1998, *available at* <<http://www.bxa.doc.gov/PRESS/98/1230Encryption.html>>. See also Encryption Items, 63 Fed. Reg. 50516 (Sept. 22, 1998); Hal Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, § 3.3.1 (Operational Costs) (Final Report, May 27, 1997) , *available at* <http://www.crypto.com/key_study/report.shtml> (concluding that it "remains unclear whether the high-risk, high-liability business of operating a key recovery center, with limited consumer demand to date, will ever be economically viable").

Compare the Canadian policy: "Fourth, we will continue to implement cryptography export controls within our commitments to the Wassenaar Arrangement; *however, we will ensure that Canadian cryptography manufacturers face a level playing field - our controls will take into account the practices of other countries so that Canadian manufactures will not be at a competitive disadvantage.*" Comments of Michael Power, Asst Dir.-Policy, Interdepartmental PKI Task Force, CIO Branch, Treasury Board Secretariat, Government of Canada (emphasis added) (on file with author).

See Remarks of U.S. Secretary of Commerce William M. Daly, at the OECD Ministerial Conference on Electronic Commerce, *A Borderless World: Realising the Potential of Global Electronic Commerce* (Ottawa, Oct. 8, 1998), OECD Doc. SG/EC(98)14/REV5 [hereinafter OECD Ministerial Conference] (noting that "[n]inety percent of our computer infrastructure is in private hands. So as policy makers, we must always keep in mind the cost of our actions"), *available at* <<http://www.oecd.org/>>.

612 organizations such as the World Trade Organization (WTO)⁸² and the Organization for
613 Economic Co-operation and Development (OECD).⁸³

614

615

PART 2

616

OPEN AND CLOSED SYSTEMS

617 As I mentioned previously, there is debate concerning whether “closed” or “open”
618 PKIs are more viable and legally efficacious for secure e-commerce and concerning
619 which model is “winning” in the marketplace.⁸⁴ The debate is unproductive and circular
620 for a number of reasons, including the fact that the terms *open PKI* and *closed PKI* are
621 generally misunderstood and ill-defined. Despite common misperceptions to the contrary,
622 the following facts about open PKI can be amply documented:

623

- 624 a. the growth and utilization of open PKIs is accelerating dramatically,
625 providing added value to the e-commerce marketplace⁸⁵;
- 626 b. open PKIs can uniquely exploit the availability of the predistributed,
627 embedded root keys of recognized certification authorities contained in
628 ubiquitously deployed browsers and other end-user software, thus better
629 providing a feature critical to many customers -- interdomain interoperation;

⁸² The WTO has endorsed a programme of work on global electronic commerce, and its Goods Counsel has set March 31, 1999, to finalize rules on how electronic commerce should be treated under WTO rules on trade in goods. See World Trade Organization, Declaration on Global Electronic Commerce (May 20, 1998), available at <<http://www.wto.org/wto/anniv/ecom.htm>>.

⁸³ <<http://www.oecd.org>>.

⁸⁴ For example, at the UNCITRAL Working Group on Electronic Commerce, although the U.S. delegation went so far as to state that e-commerce has retreated from open PKIs and that the clear trend is toward closed models, this issue is in fact hotly debated in certain PKI-related e-mail lists and elsewhere and the delegation’s statement is premature. See *infra* “Acceleration of Open PKI.”

⁸⁵ These include lower cost when using the Internet infrastructure rather than traditional leased circuit telephony, enabling of *single sign-on* rather than multiple UserID/password solutions, decreased costs for couriers (due of the enhanced security and support for nonrepudiation offered by PKI), enhanced integration of businesses and customers and improved customer satisfaction, the enabling of new applications, and greater opportunities for interoperability. See THE RADICATI GROUP, INC., PUBLIC KEY INFRASTRUCTURE SECURITY: PRODUCTS AND SERVICES, at 11-13 (1998), available at <<http://www.radicati.com>>. Cf., “Account Authority Digital Signature Model” (AADS) described at <www.garlic.com/~lynn/>.

- 630 c. open PKI provides for much lower entry and vendor-switching cost – a
631 major benefit to consumers;
- 632 d. although other PKI architectures may be better suited to particular
633 applications, open PKIs are nevertheless increasingly supplementing closed
634 PKIs, to the undeniable benefit of the user community;⁸⁶ and
- 635 e. closed and open PKIs are ultimately subject to many of the same threats,
636 vulnerabilities and liabilities – thus, closed PKIs may offer only marginal
637 security advantages.

638 The advantages of open PKI are well understood by government agencies,
639 technologists, and program managers alike and are a fundamental requirement of many
640 ongoing PKI system developments. For example, the General Services Administration’s
641 ACES (Access Certificates for Electronic Services)⁸⁷ program seeks to provide an open
642 PKI that will provide digital certificates to citizens and businesses to promote secure
643 electronic access to government information and services.

644 **The Definitions Problem**

645 Perhaps the greatest problem that has plagued the debate over open versus closed
646 PKI is the lack of a common understanding of these concepts. There is an unfortunate,
647 sometimes clashing mix of technical, marketing, and legal concepts surrounding the
648 definitions of *open PKI* and *closed PKI*.⁸⁸ As discussed below, there are many dimensions
649 to these two terms, touching on architectural, technical, competition, and contract law
650 considerations.

651

652 The focus of the controversy is on whether the users of a PKI are contractually
653 bound to rules governing its use. Potential different types of PKIs, based on such rules,
654 include the following:

655

- 656 • *Pre-existing privity PKI*: A PKI in which all intended relying parties are under privity
657 of contract (*i.e.*, have a direct contractual relationship) with the certification authority

⁸⁶ “*Global public community* - This model is achieved by extending the horizons of the community-of-interest structure with a view to encompassing the needs of many constituent communities and many applications. The model will take time to evolve, but it can possibly be built upon the services of large public PKI service operators that tailor their practices and rules to global interoperability and with the public interest in mind.” Baum & Ford, *supra* note 3, at 377.

⁸⁷ See <www.gsa.gov/aces/final/fin_rfp.html>.

⁸⁸ Because of the vigor of the debate, perhaps almost *any* proposed definitions may amount to “fighting words” within certain segments of the PKI community. See *generally supra* Part 1.d (concerning definitions).

658 (or an affiliated registration authority) prior to the *issuance* or *use* of certificates.⁸⁹
659 Here, the certification authority and its subscribers are typically part of one or more
660 defined legal entities (including perhaps a confederation of entities that have agreed
661 to adhere to the applicable rules governing the PKI). In such a PKI, users are
662 contractually constrained from sending (some or any) message to anyone outside the
663 group (and sometimes to receiving messages from outside the group as well).

664 • *Real-time privity PKI*: A PKI in which relying parties are under privity of contract
665 with the certification authority (at least) just prior to *relying* on its certificates.⁹⁰
666 Certification authorities often contemplate that the certificates they issue will be used
667 by other distinct legal entities besides a particular community's membership (or are
668 potentially enabled for such uses). Real-time privity is often undertaken and provides
669 particular advantages in PKIs that have embedded "predistributed root keys," (such as
670 those contained in most browsers,⁹¹) made publicly available to verify digital
671 signatures.

672 • *Non-privity PKI*: A PKI in which the intended relying parties are not under privity of
673 contract with the certification authority or otherwise constrained in their use of the
674 PKI. Nonetheless, to some extent, recognized usages of trade, guidelines, codes of
675 conduct, "gap-fillers," current law, and the increasing numbers of PKI laws and
676 regulations may provide a modicum of certainty (albeit inadequately) regarding such
677 PKIs.⁹²

678 ***The three positions set forth above should be viewed as points on a continuum***
679 ***rather than as absolutes.*** There are infinite variations possible in between these positions
680 that possess attributes of one or more of them to varying degrees. This is the reason that
681 this paper frequently refers to *more* open PKI rather than to open PKI in absolute terms.
682 Accordingly, the word "open" in the term *open PKI* should be construed as "more open,"
683 as opposed to "absolutely and completely open."

⁸⁹ Also, some PKIs require subscriber assent to relying party obligations at the time of initial enrollment for a certificate. To the extent that subscribers to a PKI use certificates from that same PKI (as relying parties of other subscribers), they can be contractually bound to the applicable system rules (where they have agreed to a subscriber agreement that included relying party obligations).

⁹⁰ This model is discussed further below in the context of *signing ceremonies*.

⁹¹ The growth of such predistributed keys and their effect on secure e-commerce are discussed below in "Fading Boundaries Between Closed and Open PKI."

Ironically, some pundits have claimed that "closed" PKIs are more "open" to the extent that users of closed PKIs can place their own roots into operation. Nonetheless, such an approach simply cannot scale to support many applications.

⁹² Tom Vartanian, presentation to SecureCard/SecureTech (San Jose, Dec. 9, 1998) (noting the availability of tort principles in non-privity PKI relationships).

684

685 There are other meanings to *open* and *closed* that have not been at the center of
686 the debate but have added to the confusion because of their information-technology
687 focus. These include:

688

- 689 • *Open networks and systems*: These are networks or systems that support an
690 applicable standard, such as OSI;⁹³ and
- 691 • *Competitive open PKI*: A scheme designed to ensure competition within the
692 PKI marketplace.⁹⁴

693 **The Acceleration of Open PKI - Another Dimension**

694 The clear direction in PKI is toward more open systems and interoperability,⁹⁵
695 encouraged by the global distribution and use of browsers that contain the embedded
696 roots of trustworthy certification authorities. It is the “openness” of this infrastructure

⁹³ “OSI” or “Open Systems Interconnection,” has been called “an international effort to facilitate communications among different manufacturers and technology.” MARSHALL T. ROSE, THE OPEN BOOK 613 (1990). See the OSI Basic Reference Model (ISO/IEC 7498-1), which provides for standardized protocol layering. “The open-system concept represents the buyer’s reaction to many years of lock-in to individual computer and communications hardware and software vendors. It is seen as the path to open choice of vendor for separate system components, with confidence that components from separate vendors will readily work together to satisfy a buyer’s needs. The open-systems drive is tied to the establishment and widespread implementation of standards.” RICHARD STALLINGS, DATA AND COMPUTER COMMUNICATIONS 386 (1985); see WARWICK FORD, COMPUTER COMMUNICATIONS SECURITY 7 (1994) (explaining that open does not imply any particular systems implementation, technology or means of interconnection).

"Any Electronic Signature capability should ideally be able to serve several distinct needs at the same time related to different and independent applications or service providers. It should ideally provide the capability of being a universal information and communication carrier, allowing mobile interworking using an *open* systems approach." DG XIII, Commission of the European communities, Reflection Note on Possible Collaboration in the field of Electronic Signature the key to Mobility 2, RA920007 (May 27, 1992) (emphasis added).

⁹⁴ For example, compare various regulatory schemes designed to ensure competition in local telephone markets, such as the Telecommunications Act of 1996.

⁹⁵ See Baum & Ford, *supra* note 3, at 359. Of course, it should also be noted that in many contexts, closed PKIs serve a useful purpose.

697 that is its strength and that has catalyzed its growth.⁹⁶ As Frank Gens, senior vice
698 president of Internet Research for the International Data Corporation, has stated, "[o]pen
699 PKI is a strategic imperative for enterprises as they move to secure mission-critical
700 business applications throughout their organizations."⁹⁷ This is due in part to the fact that
701 a large closed system may require much of the infrastructure required for an open system.
702 The economics of deploying a closed PKI with non-ubiquitously deployed end-user
703 software are prohibitive: "the largest cost component is from acquiring and deploying
704 PKI PC client software products"⁹⁸ (that is, the cost of proprietary client software
705 products other than "standard" globally deployed—and typically inexpensive or free—
706 browsers and related software).⁹⁹

707

⁹⁶ As organizations continue to expand use of the Internet for business-critical applications such as supply chain management, enterprise resource planning, virtual private networking, and electronic forms signing, they will require the ability to secure these applications using digital certificates within an open PKI. An open PKI allows enterprises to choose best-of-breed solutions to secure new or legacy applications—including software based on open standards; a range of implementers, including ISVs, in-house developers, systems integrators (SIs), and value-added resellers (VARs); and PKI software and infrastructure from a range of providers—while leveraging existing Internet components such as browsers, servers, routers, and firewalls. By deploying applications within an open PKI, enterprises can gain broad interoperability, rapid time-to-market, significant cost savings, and scalability across intranet, extranet, and Internet commerce applications—benefits unattainable with proprietary, stand-alone PKI software.

⁹⁷ Statement of Frank Gens, Senior Vice President of Internet Research, IDC (July 21, 1998) (on file with author).

⁹⁸ Jim Hurley, Aberdeen Group, Inc., *Evaluating the Cost of Ownership for Digital Certificate Projects* (Sept. 20, 1998), available at <<http://aberdeen.hnt.com/ab%5Fabstracts/1998/05/98050131.htm>>.

⁹⁹ There is also, necessarily, only a limited number of widely recognized trustworthy roots: "The biggest problem with the current [sic] is that the ABAecom root is not in browsers. This will cause visitors to bank web sites to receive a warning message indicating that the root is unknown or untrusted. Proposals have been made to solve this problem in the short term, including distribution of browsers on CD-ROM with the root. This is infeasible due to cost and distribution. Long term, the root in the browser from Netscape and Microsoft is the only answer. This may take six to twelve months to reach sufficient penetration of the user marketplace." Thomas Greco, President, ABAecom, *New SiteCertain Proposal* (Oct. 12, 1998) (on file with author).

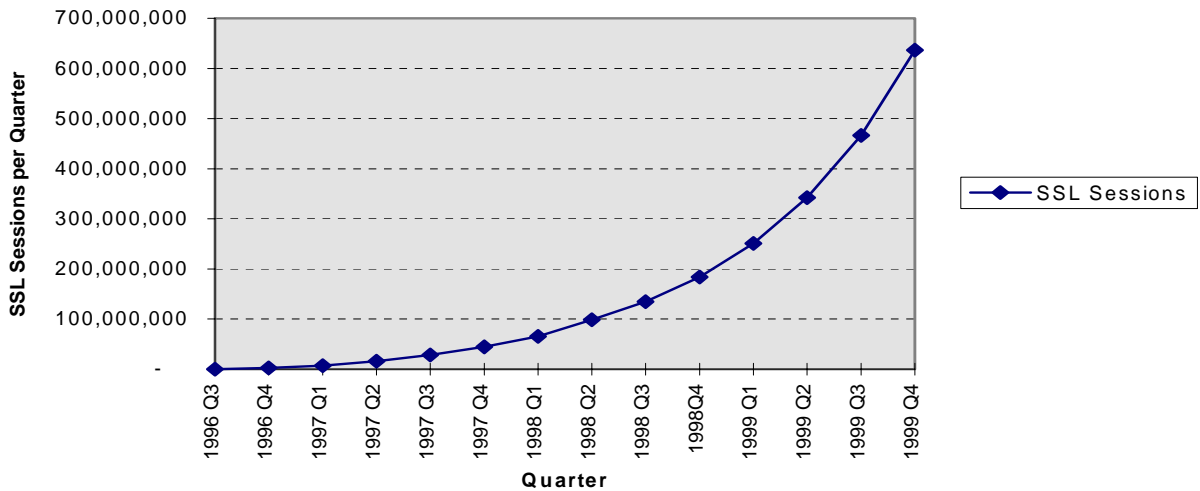
The "legacy system" issues manifested by older browsers – create a tendency to delay upgrading of browsers because of technical upward compatibility issues. The consequence of such a delay further impedes the ubiquitous distribution of new versions of browsers containing new roots.

708 One compelling example of the dramatic success of open PKI is the ubiquitous
709 use of the SSL (Secure Sockets Layer) protocol over shared paths such as the Internet for
710 e-commerce.¹⁰⁰ As demonstrated in Figure 2, today tens of millions of SSL sessions are
711 executed annually to enable secure home banking and diverse other forms of e-
712 commerce. The list of information technology companies that support this protocol is
713 comparably huge and includes a *Who's Who* of the Internet, including Amazon.com,
714 AOL, Microsoft, and Visa. Furthermore, this protocol is an open international and ANSI
715 standard (which the National Institute of Standards and Technology (NIST) claims to
716 support). As the predominant Internet security protocol for PKI and secure Internet
717 commerce, a policy that ignores the uses of SSL or downplays its importance may hurt
718 U.S. competitiveness.

719

¹⁰⁰ SSL protects communications of any application that operates over TCP. [Note RSA's recent inclusion in the DSS. See FIPS 186-1 (1999) available at <<http://www.csrc.nist.gov/fips/>>.]

SSL Sessions/Quarter



720

721 **FIGURE 2-TOTAL PROJECTED SSL SESSIONS IN THE US BASED ON PUBLIC ROOTS¹⁰¹**

722

723 Another important Internet draft standard called S/MIME¹⁰² could enable secure,
 724 authentic and confidential email communications among parties on the Internet who are
 725 not in privity. This vision could only be realized through an implementation strategy
 726 based on an open PKI architecture.

727

¹⁰¹

Period	Projected Growth	Total Sites (Industry)	# Sessions/Site/Quarter (est.)	Total Sessions
1996 Q3		486	600	291,600
1996 Q4		3830	660	2,528,064
1997 Q1		9676	726	7,024,486
1997 Q2		20366	799	16,264,607
1997 Q3		32426	878	28,485,295
1997 Q4		46226	966	44,668,848
1998 Q1		61274	1063	65,130,802
1998 Q2		84019	1169	98,237,557
1998 Q3		104790	1286	134,776,517
1998 Q4	24%	129940	1415	183,835,170
1999 Q1	24%	161126	1556	250,751,171
1999 Q2	24%	199796	1712	342,024,598
1999 Q3	24%	247747	1883	466,521,551
1999 Q4	24%	307206	2071	636,335,396

¹⁰² See <<http://www.ietf.org/ids/by.wg/smime>> (describing S/MIME).

728

The Fading Boundaries Between Open and Closed Systems

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

Open systems are purportedly inferior to closed systems because they operate without the contractual assent of relying parties. As noted above, the claim is that relying parties are not in privity with the certification authority (or affiliate registration authority) and thus are not bound to applicable system rules -- anyone can obtain and rely on certificates or purportedly “surf over” and use a system without being obligated to honor its rules.

A closer look at “open” PKIs in actual commercial practice demonstrates a very different reality, however. Open PKIs often become *constrained*,¹⁰³ or bounded, just prior to use by relying parties. For example, systems that require relying parties to agree to a “relying party agreement” or “system rules” (typically by *click wrap*¹⁰⁴) prior to providing them with certificate status information can as a matter of practice invoke relying party privity, thereby legally binding users.¹⁰⁵ This practice provides advantages over closed PKIs, such as enabling a broader class of users (with attendant broader market reach) than would be available within a closed system.

Thus claims that open PKIs are being “eclipsed” by closed systems miss the mark; rather, more open PKIs have sometimes adopted certain closed-system attributes while retaining their own inherent advantages. The upshot is that open systems both promote ubiquitous e-commerce *and* allow for procedures and practices that bind or otherwise constrain relying parties.

Furthermore, intranets and extranets (generally understood as manifestations of closed systems) are being deployed to leverage the benefits of Internet commerce. Working in an isolated island is often impractical and strategically limiting.¹⁰⁶ There are

¹⁰³ See BAUM & FORD, *supra* note 3, at 376.

¹⁰⁴ “Click wrap” or “Web wrap” is the Internet version of shrinkwrap (a method of seeking to bind software purchasers by opening the shrinkwrapped package). The adequacy of shrinkwrap was favorably treated in the case *ProCD v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996). However, the law in this area remains uncertain, including with regard to the proposed U.C.C. Art. 2B.

¹⁰⁵ See *infra* Part 4 on relying party obligations.

¹⁰⁶ One example of this trend is evident at VeriSign, where both “closed” (or “private label”) and “open” (or VeriSign Trust Network) PKIs are offered. Enterprise customers have (with increasingly frequency) chosen an open solution to ensure global interoperation. Also, increasing demand for interoperation among *communities of interest* suggests that such communities agree on common principles and practices that may be well-beyond the scope and level of compatibility of closed PKI applications, thus creating larger or more open closed PKI applications.

754 also many new kinds of intermediaries, such as Web-based auction services and
755 securities brokerages, that are successfully exploiting open-systems electronic
756 commerce.¹⁰⁷ Further, there is also a trend for closed PKIs to increasingly interoperate in
757 various ways, including via interdomain gateways and cross-certification.¹⁰⁸ Finally, we
758 can imagine “on the fly” creation and termination of communities of interest, a capability
759 with many potential benefits and for which there is increasing demand, recognizing that
760 community formation is increasingly fluid in contemporary society. Such temporary
761 communities (forming, for example, around particular political issues) will grow as the
762 technical mechanisms to support them become available.¹⁰⁹

763 **Common Threats**

764 Some government representatives claim that closed PKIs do not share many of
765 the same liability risks as open PKIs regarding third-party injuries, because only
766 subscribers or members of a closed community (persons who have been contractually
767 bound to applicable system rules) have access to the community’s certificates and
768 messages, and thus third parties cannot be affected. Upon closer scrutiny this theory has
769 been marginalized. Certificates and corresponding secured messages can “leak” from a
770 closed system.¹¹⁰ That is, certificates intended for exclusive use within a closed

¹⁰⁷ See Steve Levine, Product Marketing Sr. Dir., Oracle Corporation, Remarks at the *Electronic Commerce and the Global Economy Conference* (Wash. DC, Aug. 24, 1998).

¹⁰⁸ As PKIs increasingly interoperate, the consistency of their “core” practices will harmonize increasingly and move towards a virtual open global PKI of PKIs. This phenomenon parallels aspects of the interoperation within the electronic messaging and general Internet space. For example, see Internet Engineering Task Force (IETF), *Requests for Comment (RFC’s)* (regarding proper conduct on Internet and email usage), available at <<http://www.rfc-editor.org/overview.html>>.

¹⁰⁹ See, e.g., Microsoft’s *Netmeeting* application, available at <<http://www.microsoft.com/netmeeting>>.

¹¹⁰ See Dwight Arthur, *Certificate Leakage* (June 18, 1998), available at <<http://dwightarthur.home.mindspring.com/leakage>>. The implications of the Net were also considered in *Trust in Cyberspace*:

To a first approximation "everything" is becoming interconnected. The June 1997 Pentagon cyberwar game Eligible Receiver (Gertz, 1998; Myers, 1998) demonstrated that computers controlling electric power distribution are, in fact, accessible from the Internet. It is doubtless only a matter of time before the control network for the public telephone network is discovered to be similarly connected -- having just one computer connected to both networks suffices. Thus, the Internet will ultimately give ever larger numbers and increasingly sophisticated attackers access to the computer systems that control critical infrastructures. The study committee therefore concluded that resisting attack is a dimension of trustworthiness that, although not a significant source of

771 community can escape and be used by relying parties who are not in privity with the
772 issuing certification authority.

773

774

PART 3

775

MINIMALIST LAWS

776

777 There is considerable support for what is best described as “minimalist”
778 legislation in the area of e-commerce. This approach essentially argues that all that is
779 needed or desirable is legislation that allows electronic records and signatures to suffice
780 in place of their traditional written counterparts.¹¹¹ This approach is the end product of
781 more than a decade of active effort to get various legal regimes to accept electronic
782 commerce.

783

784 But will a minimalist law satisfy the needs of secure e-commerce? Consider the
785 need for secure interoperability, a fundamental requirement of effective e-commerce. To
786 achieve interoperability, particularly within a secure system, it is crucial to specify
787 implementation criteria and to do so at a level more detailed than abstract policy can
788 possibly provide. For example, in establishing system requirements it may be acceptable
789 to specify merely that “secure e-mail” is required, but actual implementation will be
790 delayed unless the applicable procedural rules are identified and it is clarified whether
791 commercial security algorithms using the secure/multipurpose Internet mail extension
792 (S/MIME) protocol¹¹² or government algorithms using the Message Security Protocol

disruption today, has the potential to become a significant cause of outages in the future.

Supra note 51, at ch. 1.

¹¹¹ And yet, California’s technology-neutral “electronic signature” regulation could theoretically become a very lengthy document because it is structured to accommodate a theoretically infinite number of “alternative technologies” to be comprehensively listed in an appendix. *See* CAL. GOV’T CODE § 16.5, available at URL cited *supra* note 34; CAL. CODE REGS., tit. 2, §§ 22000 *et seq.*, available at URL cited *supra* note 24. The obsessive focus of some commentators on the length of e-commerce rules has become somewhat theological. Length is considered unacceptable by some minimalists, no matter the content, purpose and practical need of the rules. Ironically, in almost every instance where digital signatures have been the subject of statutory treatment, corresponding detailed regulations were determined necessary for proper implementation. Note: a number of minimalist supporters have taken these positions because they believe that rules development, at this early state, may be premature because market development does not justify it.

¹¹² *See supra* note 102.

793 (MSP),¹¹³ or both, will prevail.
794

795 Moreover, for secure e-commerce to advance, the security services employed
796 must enable mainstream implementations (in terms of protocols, standards, applications,
797 tools, rights and obligations of the parties, etc.).¹¹⁴ Digital certificates provided by an
798 open PKI constitute the only device that enables all of the security services necessary to
799 enable global secure interoperability (as well as biometrics, incidentally), in standards-
800 based implementations and for a wide range of commercial off-the-shelf applications. All
801 other security mechanisms and technologies, including biometrics, may be capable of
802 providing a single security service or a limited range of services but lack the requisite
803 features to enable open e-commerce. Thus the various ongoing initiatives seeking to
804 define policy in a technology-neutral manner may continue to be fundamentally
805 inadequate.¹¹⁵

¹¹³ See <http://www.armadillo.huntsville.al.us/Fortezza_docs/missi1.html#specs> (describing MSP).

¹¹⁴ Such implementations should be consistent with the long tradition of voluntary self-regulation and private, third-party oversight mechanisms such as rigorous audits by certified public accountants using generally accepted auditing criteria (*e.g.*, the Statement of Auditing Standards 70 (SAS 70) promulgated by the American Institute of Standards and Technology <<http://www.aicpa.org>>). The California Digital Signature Regulations provide: “The Secretary of State shall place a CA on the ‘Approved List of CAs’ after providing the Secretary of State with a copy of an unqualified performance audit performed per standards set in the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards 70 (S.A.S. 70) ‘Reports on the Processing of Service Transactions by Service Organizations’ (1992) to ensure the CA’s practices and policies are consistent with the CA’s stated control objectives.” CAL GOV’T REGS., tit. 2, § 22003(a)(6)(C).

In addition, the more recently developing framework and criteria for the evaluation and approval of certification authorities provides another developing means of oversight and regulation. *See, e.g.*, INFORMATION SECURITY COMMITTEE, AMERICAN BAR ASSOCIATION, PKI EVALUATION GUIDELINES (currently being drafted), *available at* <<http://www.abanet.org/scitech/ec/isc/home.html>>. *See* Charles Merrill, *The Accreditation Guidelines: A Progress Report on the Work in Process of the ABA Information Security Committee*, 38 JURIMETRICS J. 345 (1998). Nonetheless, there remains a lack of *global* standards. Consequently, technology neutral (or even minimalist technology-specific laws) may prove to be inadequate to avoid inherent obstacles to market access.

It may neither be possible nor desirable to prevent sector-specific legislation. Nonetheless, if such legislation is unavoidable, hopefully it will at least consider the developing approach to multisector legislation, to best ensure inter-sector interoperability.

¹¹⁵ For example, consider the technology-neutral rule contained in Article 7 of UNCITRAL’s

806

807

UNCITRAL

808

809

810

811

812

813

814

815

At an earlier period in the development of electronic commerce law and with respect to general underlying rules, a “technology-neutral” international e-commerce law, the U.N. Model Law on Electronic Commerce (the *UNCITRAL Model Law*), was adopted in 1996 by the United Nations Commission on International Trade Law (UNCITRAL).¹¹⁶ UNCITRAL has since focused on the development of a model law on “electronic signatures,” with an initial emphasis on digital signatures and PKI. Nonetheless, there is a movement afoot to make the proposed uniform rules on electronic signatures technology neutral.¹¹⁷ With a successful model law on electronic commerce complete and

MODEL LAW ON ELECTRONIC COMMERCE (1998) [hereinafter UNCITRAL MODEL LAW], available at <<http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm>>. “This rule, while helpful, left a lot to the judgment of the parties involved in electronic commerce” Amelia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform*, 72 TUL. L. REV. 1931, 1969 (1998).

One advocate for Internet regulation argues that a hands-off approach by government is “naïve libertarianism.” Phil Leggiere, *Constitutionalist in Cyberspace*, PENN. GAZETTE, Nov./Dec. 1998, at 48 (interviewing Prof. Larry Lessig, Harvard Law School). Other critics contend that the government has engaged in inappropriate “selective regulation” – such as failing to address Internet privacy while over-regulating cryptographic export controls and intellectual property. Marc Rottenburg, Esq., EPIC, Presentation at the OECD Ministerial Conference, *supra* note 81.

See MICHAEL K. KELLOGG ET AL., AN INDUSTRY IN TRANSITION (1992) (arguing that “[t]he shift from managing monopoly to managing competition is accelerating, however, and it is one of the great, if unheralded regulatory initiatives of our day”).

¹¹⁶ UNCITRAL MODEL LAW, *supra* note 115.

Also, some business applications are highly dependent, in fact, inherently based on PKI, such as those undertaken via the Secure Electronic Transactions (SET) standard and various “e-cash” applications.

¹¹⁷ This push towards technology-neutrality has been so far been supported by the U.S. Delegation. Another delegation (Singapore) suggested that “[t]he focus of the project has turned from looking for remote, faceless means of identification to finding rules of attribution generally for all forms of electronic signatures. This probably means that the group does not think it is appropriate to make international harmonized rules on PKI as a form of remote, faceless identification system. This seems to have been largely due to the perception in the group that many uses of DS technology do not involve total strangers transacting without having previously established off-line contact.” Email from Khang Chau Pang, Esq., to Michael S. Baum (Sept. 3,

816 increasingly implemented (in whole or in part),¹¹⁸ however, the benefit of promulgating
817 yet another, “technology-neutral” e-commerce uniform rules on electronic signatures
818 would seem questionable at best.¹¹⁹ As Professor Mads Andersen, head of the Danish
819 delegation and work group chair, states:

820

1998) (on file with author). This is likely a manifestation of the confusion about open versus closed systems. *See* discussion *supra* regarding describing open versus closed PKI.

Actually, a technology-neutral approach was included in UNCITRAL’s terms of reference for the Working Group while at the same time retaining a number of technology facilitating provisions.. Technology neutrality was not interpreted to exclude specific provisions along with more general provisions. “Consistent with the mandate received from the Commission and with views expressed at the thirty-second session of the Working Group (*see* A/CN.9/446, ¶¶ 4 and 45), the purpose of the draft article is to ensure the media-neutrality of the Uniform Rules, [and] to make it clear that the use of low-security authentication techniques is not prohibited.” U.N. Doc. A/CN.9/WG.IV/WP.76, ¶ 21, at 10 (May 25, 1998) [hereinafter UNCITRAL Draft Uniform Rules], *available at* <http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-76.htm>.

¹¹⁸ The *UNCITRAL Model Law* has recently been experiencing global “uptake,” having been adopted or integrated into legislation in Singapore, *see* Singapore Electronic Transaction Bill, *supra* note 12, and favored in bills in Australia, *see Electronic Commerce: Building the Legal Framework* (1998), *available at* <<http://www.law.gov.au/aghome/advisory/eceg/ecegreport.html>>, Colombia, *see* Draft Proposal of Law on Electronic Commerce, Digital Signatures and Certification Authorities *available at* <http://www.qmw.ac.uk/~tl6345/colombia_en.htm>, and even a few U.S. states, including Illinois, *see* the Illinois Electronic Commerce Security Act.

¹¹⁹ To the extent that “the UNCITRAL Model Law on Electronic Commerce will have a greater impact on developments in United States domestic commercial law than either the UNCITRAL Convention on the International Sale of Goods or the UNIDROIT Principles on International Commercial Contracts,” Boss, *supra* note 115, at 1931, we face the uncertainty of case law (particularly in the absence of technology-specific legislation).

To be a technology neutral law it must remain up in the clouds...[and] would force the [Working Party on Electronic Commerce] to avoid addressing the real issues.” Remarks of Khang Chau Pang, State Counsel, Republic of Singapore (Nov. 5, 1998, Vienna) (on file with author).

This issue rings of the many concerns of the EDI legal community regarding the “octogenarian judge problem” – that is, concern that an elderly or technophobic judge would not give electronic data due consideration and enforceability.

821 [A technology-neutral approach] has yet to prove its justification. Although
822 the idea was to make the text "future resistant" (which might indicate a more
823 general and fundamental approach that does not cling to specific technologies), it
824 has led to a much more complicated text. It is my personal belief that the
825 [working group] will face substantial difficulties for the following reason: If you
826 want to maintain technology neutrality to its extremes, you end up with a
827 document so basic that it only repeats the [UNCITRAL Model Law] (in which
828 case we will be wasting our time, since we already did that). If on the other side
829 you want to take all different—existing and future—technologies into account,
830 you will—as [UNCITRAL’s Working Group on Electronic Commerce] tries to
831 now—have to give specific rules for each and every individual technology,
832 which (1) is extremely difficult and (2) anyway may lower the "future resistance"
833 towards future technologies that we do not yet know of. And in that case you will
834 also be wasting your time.¹²⁰

835

836 As to the future of the UNCITRAL draft uniform rules on electronic signatures,
837 another international policy expert has stated that, from a “legal science approach,” the
838 claim that we harm other techniques by providing rules on digital signatures “doesn’t
839 float and obviously is not an argument that can be used with any convincing value. Are
840 we giving up on electronic signatures? The current draft is already fairly neutral in my
841 view. I don’t see what more you can do to introduce neutrality.”¹²¹

842 **Proposed Convention**

843 In May 1998, the U.S. delegation to UNCITRAL, under the leadership of the U.S.
844 Commerce and State Departments, initially proposed that, rather than pursue the drafting
845 of a uniform rules on electronic signatures, UNCITRAL should draft only a convention
846 based on the more general *UNCITRAL Model Law on Electronic Commerce*,¹²² in order to

¹²⁰ Email from Prof. Mads Andersen to Michael S. Baum (Aug. 10, 1998) (on file with author) [hereinafter Andersen Email]. Professor Andersen served as Chairman of the UNCITRAL Working Group on Electronic Commerce. The California treatment of signature dynamics is more of a specific vendor’s product specification than it is a “neutral” enabling rule.

¹²¹ Telephone interview of the Hon. Renaud Sorieul, Sr. Legal Officer, UNCITRAL, by Michael Baum (Vienna, Aug. 18, 1998) (on file with author) [hereinafter Sorieul Interview].

¹²² See Proposal by the United States of America, *Draft International Convention on Electronic Transactions*, U.N. Doc. A/CN.9/WG.IV/WP.77 (May 25, 1998), available at <<http://www.un.or.at/uncitral/english/sessions/wg-ec/wp-77.htm>>. The proposal stated that “[a]ny rules should neither require nor hinder the use or development of authentication technologies. States should anticipate that authentication methods will change over time and avoid legislation

847 promote basic e-commerce rules on a minimalist basis and to accelerate the likelihood of
848 adoption by the states. Some countries interpreted this as an effort to forestall
849 proscriptive legislation. Another goal was to advance party autonomy.¹²³ The U.S.
850 delegation later agreed to a two-track approach: to pursue simultaneously the drafting of
851 a technology-neutral convention and the continuation of the current UNCITRAL drafting
852 project on electronic signatures. That approach is only now being seriously considered by
853 other delegations, a number of which are concerned with the likelihood that the two-track
854 approach will complicate and slow UNCITRAL's current rule-making efforts. The
855 convention proposal has yet to gain adequate support.¹²⁴ The U.S. and a few other

that might preclude innovation or new applications. States should avoid laws that intentionally or unintentionally drive the private sector to adopt only one particular technology for electronic authentication to the exclusion of other viable authentication methods." *Id.* Upon adoption of a convention by a country, it would become bound to the entire convention but for any explicitly stated exceptions.

Also, concern remains that drafting another technology neutral law may re-open the *UNCITRAL Model Law*, cited above in note 111 – and it is thought that the likelihood of reaching agreement today is considerably less than it was in 1996 (when the *UNCITRAL Model Law* was enacted).

¹²³ See text *infra* at notes 167-168 (on party autonomy). Note that before the implementation of U.C.C. Art. 4A (Funds Transfers), "it was estimated that only ten percent of the transfers – in terms of dollars – were governed by a private contract between the bank and the customer." Carlyle C. Ring, Jr., *The UCC Process--Consensus and Balance*, 28 LOY. L.A. L. REV., 287, 293 (Nov. 1994). Query the extent to which contract (as facilitated through enhanced party autonomy) will assure adequate coverage in the e-commerce arena in light of Mr. Ring's assertion of only 10% coverage in the funds transfer arena. This may suggest a corresponding need for rules governing secure electronic commerce.

See the various joint statements on electronic commerce such as between the U.S. and Australia, <<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/12/2/10.text.1>>, and between the U.S. and Ireland, see *Communique*, *supra* note 28.

¹²⁴ It was apparent that UNCITRAL's resources, including the time commitments of the delegations, were so constrained that such parallel development was an unrealistic expectation. "It is quite clear that there is an overwhelming majority of people and delegations within the UNCITRAL WG who supports this view." Andersen Email, *supra* note 120.

Other delegations have privately opined that perhaps it was "insufficient preparation" of the proposed convention that slowed its acceptance and that it may also have been a failure of its proponents to cogently explain its agenda, philosophy, motivations, and politics.

In addition, the International Chamber of Commerce (ICC) has urged that UNCITRAL "[a]dvance *product / implementation-neutral* rather than technology-neutral rules – at least until any non-asymmetric cryptographic technology is demonstrated to provide sufficient and

856 delegations continue to advocate a technology-neutral convention (although many of the
857 convention’s underlying positions are widely supported).

858

859 Subsequently, at an informal meeting to review the draft convention, the proposed
860 technology-neutral section of the draft was discussed.¹²⁵ Most participants supported
861 moving it into a preamble (where it would have merely a prefatory effect) rather than
862 keeping it as an operative provision.¹²⁶

863

864 **“Embrace and Extend”**

865 The notion of advancing a technology-neutral convention *instead* of PKI model
866 rules is troubling because if international PKI model rules are not developed, then
867 national governments will not have a practical model on which to base their own PKI
868 laws and self-regulation systems. And governments *are developing and will continue to*
869 *develop* PKI-specific rules!¹²⁷ Thus, failing to draft an international PKI model law will
870 potentially produce a legacy of infinitely diverse, non-interoperable laws—a true
871 nightmare to advocates of a global secure e-commerce infrastructure.¹²⁸ Indeed, *those*
872 *jurisdictions that do not have a PKI-specific framework implemented or on the table will*
873 *most likely not even have a seat at the table*—they simply will not have the bargaining
874 power with other jurisdictions to effect harmonization. The result could very well be
875 worse than the status quo.

876

877 To the extent that digital signatures and PKI present the predominant underlying
878 platform for secure electronic commerce and present nontrivial technical and legal
879 challenges and economic opportunities, then specific digital signature and PKI rules
880 would be responsive to the needs of the global electronic marketplace – certainly no less
881 (and possibly much more) than would be “generic” rules to enable electronic commerce.

882

necessary Internet-compatible security services.” ICC, DRAFTING PRINCIPLES FOR UNCITRAL
WORKING GROUP ON ELECTRONIC COMMERCE (1998).

¹²⁵ Meeting sponsored by the Internet Law and Policy Forum (Vienna, Austria, Nov. 5, 1998).

¹²⁶ “How can you hope to get a state to refrain from recommending certain technology – I don’t see how any state will agree to a convention that prevents their choice.” Sorieul Interview, *supra* note 121.

¹²⁷ Two examples of such laws that have been criticized by the U.S. delegation include the German Digital Signature Law, *supra* note 9, and the Italian Law No. 59 of 15 March 1997, *supra* note 10. See also the Malaysia Digital Signature Bill 1997, *supra* note 11.

¹²⁸ See FORD & BAUM, *supra* note 20, at 370-72.

883

PART 4

884

TOWARD A MODEL PKI LAW

885

886

887

888

889

890

891

POSITION/RULES	COMMENTS
No rules	<i>No rules</i> would not even help remove basic barriers to e-commerce. Thus there is widespread agreement that this position is unacceptable and that at least some level of rules is needed to facilitate the growth of e-commerce.
Media-neutral, technology-neutral, and context-neutral rules	Media-neutral rules would abolish the old distinction between paper on the one hand and all things electronic or paperless on the other hand. The idea of technology-neutral rules is a slightly more “modern” version of this notion. <i>Context neutrality</i> is a synonymous term.
Technology-specific rules	This position would address specific technologies without necessarily ruling out the use of other technologies. ¹²⁹
Product-neutral rules	This position would allow adoption of a technology but preclude embracing a type of technology controlled exclusively by a particular vendor. This position has also been called <i>implementation-neutral</i> .
Product-specific rules	This position would sanction or mandate a particular vendor’s goods or services and is generally discouraged by all sides of the debate.

892

893

TABLE 3 - TECHNOLOGY-NEUTRAL AND OTHER POSITIONS

894

895

896

897

This continuum indicates that there are two “outer” positions (“no rules” and “product-specific rules”) that should largely be avoided in policymaking and at least three others that should be generally applied based on the relevant regulatory interests in

¹²⁹ Sorieul Interview, *supra* note 121. “Technology specific is not the opposite of technology neutral. Technology neutral is the opposite of technology favoritism.” Remarks of Khang Chau Pang (Vienna, Nov. 6, 1998) (on file with author).

898 the particular case, which might include such concerns as the nature and degree of
899 security necessary for the particular application, the public interest in ensuring enhanced
900 security, etc.

901

902 As described above, there is some support for moving PKI-specific rules toward
903 greater generality. In moving in this direction, perhaps there is still a basis for
904 constructive compromise. That is, perhaps we can modestly generalize some of the
905 detailed PKI-specific proposals while still retaining ample treatment of those PKI issues
906 that are fundamental and applicable to the security and commercial viability of diverse
907 PKIs.¹³⁰ Such rules should not only prevent legal barriers to the enforceability of PKI-
908 based transactions but also provide for the enhanced certainty and benefits PKI can bring
909 to the global e-commerce community. While “party autonomy” and other general
910 precepts should be included (because they *are* indispensable), they should also include,
911 for example: (1) obligations for key holders to exercise reasonable care to safeguard their
912 private key, (2) obligations for relying parties to check the status of certificates before
913 relying on them, and (3) provision for beneficial presumptions when using secure or
914 enhanced digital signatures. Because of the particular importance, controversy, and affect
915 of these issues on many PKI-related rules, each is considered below.

916

917 **a. Safeguarding Subscriber Private Keys**

918 The subscriber’s obligation to protect his or her private key is a feature of most if
919 not all PKI-specific rules.¹³¹ This principle is expressed within the *Digital Signature*

¹³⁰ Consideration should be given to deriving applicable principles from the *Digital Signature Guidelines*, *supra* note 20, and the International Chamber of Commerce’s *General Usage for International Digitally Ensured Commerce (GUIDEC)* (1997), available at <<http://www.iccwbo.org/guidec2.htm>>.

¹³¹ “§ 370.56 - *Negligence contributing to forged signature*. A person whose failure to exercise ordinary care substantially contributes to the creation or submission of a forged signature is precluded from disavowing the forged signature. The burden of production and the burden of persuasion is on the person against whom the signature is asserted to establish the exercise of ordinary care.” Regulations Governing Agencies for the Issue and Offering of United States Savings Bonds, Including Sales by Electronic Means; Final Rule, 63 Fed. Reg. 64544, 23695, 64554 (Nov. 20, 1998). This section of the regulation is drawn from section 3-406 of the Uniform Commercial Code (UCC). The responsibilities imposed upon persons in regard to the technology used to create and submit electronic signatures are similar to those imposed under the UCC in regard to rubber signature stamps used to sign checks. Official Comment 3 to UCC section 3-406 is enlightening in this regard. If a person’s rubber signature stamp and checks, kept in a unlocked drawer, are stolen and used by an unauthorized party to forge a check, a bank may be able to successfully argue that the person is precluded from disavowing the forged signature because the person’s lack of ordinary care substantially contributed to the forgery.

920 *Guidelines*: “[d]uring the operational period of a valid certificate, the subscriber shall not
921 compromise the private key corresponding to a public key listed in such certificate”¹³²
922 And, the most recent *Note from the Secretariat* of UNCITRAL proposes that “[a]
923 signature holder is obliged to: (a) Exercise due care to avoid unauthorized use of its
924 signature”¹³³ The related and controversial question has been the extent to which the
925 issuing certification authority should be held responsible for the consequences of a
926 subscriber’s failure to safeguard his or her private key (or, for that matter, for any
927 unauthorized use of a subscriber’s private key).¹³⁴ Some pundits have hinted that PKI
928 rules should require certification authorities to guarantee a level of consumer protection
929 that is at least equal to that provided by credit card providers. For example, one academic
930 states that

Similarly, under the proposed rule if a person fails to take adequate security precautions to protect access to electronic signature technology (such as by not safekeeping a computer password, for instance) and this failure substantially contributes to the creation or submission of an unauthorized signature, the person would be precluded from disavowing the signature.

Id. at 23699

¹³² DIGITAL SIGNATURE GUIDELINES, *supra* note 20, § 4.3. This principle is supplemented by the Guidelines’ *trustworthiness* obligations, such as stated in Section 3.1.

¹³³ UNCITRAL Draft ARTICLES, *supra* note 67, Art. F, Remarks 18-19.

¹³⁴ “§ 370.56 - *Negligence contributing to forged signature*. A person whose failure to exercise ordinary care substantially contributes to the creation or submission of a forged signature is precluded from disavowing the forged signature. The burden of production and the burden of persuasion is on the person against whom the signature is asserted to establish the exercise of ordinary care.” Regulations Governing Agencies for the Issue and Offering of United States Savings Bonds, Including Sales by Electronic Means; Final Rule, 63 Fed. Reg. 64544, 23695, 64554 (Nov. 20, 1998). This section of the regulation is drawn from section 3-406 of the Uniform Commercial Code (UCC). The responsibilities imposed upon persons in regard to the technology used to create and submit electronic signatures are similar to those imposed under the UCC in regard to rubber signature stamps used to sign checks. Official Comment 3 to UCC section 3-406 is enlightening in this regard. If a person’s rubber signature stamp and checks, kept in a unlocked drawer, are stolen and used by an unauthorized party to forge a check, a bank may be able to successfully argue that the person is precluded from disavowing the forged signature because the person’s lack of ordinary care substantially contributed to the forgery.

Similarly, under the proposed rule if a person fails to take adequate security precautions to protect access to electronic signature technology (such as by not safekeeping a computer password, for instance) and this failure substantially contributes to the creation or submission of an unauthorized signature, the person would be precluded from disavowing the signature.

Id. at 23699

931

932 [t]he desirability of technology-specific legislation should be especially suspect if
933 it comes at the expense of consumer protection provisions found in the regulation
934 of equivalent electronic financial services such as credit cards or electronic funds
935 transfers. . . If any special legislation is needed to promote sound business
936 practices in Internet commerce at this early stage in its development, it would be
937 technology-neutral consumer protection legislation, not protections for
938 technology developers and promoters before the risks associated with their
939 products have become apparent.¹³⁵

940

941 Accordingly, the “\$50 consumer liability limit” has become a standard in a
942 crusade to extend the likes of the Electronic Fund Transfer Act (EFTA) consumer
943 protection provisions¹³⁶ to all certification authorities that touch or concern consumers.
944 There are reasons why this is inappropriate economically and legally. For example, on-
945 line credit card transactions—including those transmitted over secure channels such as
946 those provided by SSL or SET¹³⁷—are most likely already covered by the EFTA’s \$50
947 liability limit. Why introduce a second, redundant set of liability regulations on
948 certification authorities? There are compelling reasons to consider the adverse economic
949 burden such obligations would place on the certification authority industry, especially in
950 light of the nascent nature of the industry. Unlimited certification authority insurance to
951 cover such consumer risk is unavailable and the potential risk to certification authorities
952 could bankrupt the industry. And there have yet to be any instances of alleged or proven
953 damages, or litigation regarding digital certificates and digital signatures, although
954 consumer use has been comparatively limited.

955

956 Additionally, the PKI industry and on-line merchants is responding to the liability
957 issues, without government intervention.¹³⁸ The PKI industry response has included
958 extended warranty programs, new insurance products, prophylactic measures, including

¹³⁵ Jane K. Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177 (1998).

¹³⁶ 15 U.S.C. §§ 1693 *et seq.* (1998); 12 C.F.R. § 205.5 (1998) [226.12] (Reg. E). *See also* the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.* (1998).

¹³⁷ SET is a comprehensive protocol and infrastructure specification to support bank card payments as part of Internet-based electronic shopping or service provision. *See* (visited Jan. 11, 1999) <[http:// www.setco.org](http://www.setco.org)>.

¹³⁸ Success with improved notice and disclosure mechanisms may forestall future regulation/legislation. *See, e.g.*, the NetSure Protection Plan (<<http://www.verisign.com/netsure>>), WebTrust (<<http://www.aicpa.org>>), and NetDocs (<<http://www.netdocs.com/>>). *See also* TRUSTe (<<http://www.truste.org>>) and the Better Business Bureau (<<http://www.bbb.org>>) (related privacy and Internet business self-regulation initiatives).

959 the introduction of inexpensive hardware tokens (chip cards) to enhance the protection of
960 private keys,¹³⁹ improved notice and disclosure mechanisms,¹⁴⁰ and the introduction of
961 new technologies and techniques to further mitigate risks to the end-user.¹⁴¹

¹³⁹ See Jennifer Hagendorf, *HP Ships PCs Equipped For Smart Cards*, TECHWEB (Oct. 5, 1998), available at <<http://www.techweb.com/infoseek/wire/story/TWB19981005S0011>> (announcing that Hewlett-Packard's corporate PCs, notebooks, and workstations will ship smart card-ready); Margaret Quan, *Fingerprint Sensor Looks To Tap Security Applications*, TECHWEB (Oct. 4, 1998), available at <<http://www.techweb.com/wire/story/TWB19981004S0001>> (describing Veridicom's joining four other semiconductor suppliers that have announced plans to manufacture chip-based fingerprint scanners and pursue similar markets and reporting that more than a dozen companies plan to announce products that will incorporate Veridicom's technology, with availability in early 1999); *New IBM Smart Card Security Kit Protects Data On Notebook PCs*, BUSINESS WIRE (Oct. 19, 1998), available at <<http://www.infoseek.com/Content?arn=BW1025-19981019&qt=RSA,+SDTI,+%22Security+Dynamics%22,+Informix,+Xerox,+Tandem,+Encryption,+Cryptography,+Authentication,+Certification,+%22University+of+Colorado%22&sv=IS&lk=&col=NX&kt=A&ak=news1486>> (announcing IBM's "new smart card security system that prevents unauthorized users from accessing information on a notebook computer").

¹⁴⁰ For example, the American Bar Association's Information Security Committee "Notice Project" is developing standardized notices and warnings for use in browsers and other end-user software addressing the operation of cryptographic functions to advance cross-sector agreement on notices and conspicuousness. See <<http://www.abanet.org/scitech/ec/isc/home.html>>.

Conspicuous in the latest draft of Art. 2B means so "displayed, or otherwise presented that a reasonable person against which it is to operate ought to have noticed or become aware of it. In the case of an electronic record intended to evoke a response by an electronic agent, a term is conspicuous if it is presented in a form that would enable a reasonably configured electronic agent to take it into account or react without review of the record by an individual." Draft U.C.C. § 2B-102(8) (Aug. 1, 1998), available at <<http://www.2bguide.com/>>. Cf. Letter from Joan Z. Bernstein, Dir., Bureau of Consumer Protection, FTC et al., to Carlyle C. Ring, Jr., Chair, NCCUSL 2B Drafting Committee, and Geoffrey Hazard, Jr., Dir., Am. Law Inst. (Oct., 30, 1998), available at <<http://www.ftc.gov/be/v980032.htm>> (commenting, on behalf of the FTC, on consumer implications of proposed Art. 2B).

¹⁴¹ Examples include as key recovery and management services, and enhanced certificate status services. Also, to the extent that "[t]rustworthiness is a systemwide attribute," then the impact (and responsibility) of CAs must be considered together with end-user software vendors and the other providers of products and services that create a PKI. See TRUST IN CYBERSPACE, *supra* note 51.

962

963 Legislators may be looking for a “way out,” from a consumer-protection
964 perspective, by trying to avoid too much contractual exemption. So it is tempting to put a
965 monolithic, simplistic minimum standard or rule in place—essentially, to follow the
966 credit card model. However, as one noted expert put it, “I think everyone would agree
967 that a \$50 cap doesn’t fit and doesn’t make sense in the e-commerce world. . . I am
968 prepared to take any [new] idea [but] I am not aware of any useful thinking [on the
969 topic].”¹⁴²

970

971 The consumer advocate arguments in the foregoing discussion would tend to
972 implicate nearly all PKI-based transactions, no matter what their intended purpose.
973 Should we be alarmed? Perhaps we should, in light of the following data -- in 1998,
974 consumer electronic commerce amounted to approximately 20 percent of all e-commerce
975 transactions (about 80 percent consisted of business-to-business transactions).¹⁴³ Of this
976 20 percent of transactions, it is estimated that 99 percent were settled by credit card.
977 Thus, less than 1 percent of consumer e-commerce transactions did *not* involve credit
978 cards.¹⁴⁴ How could it make sense to impose a monolithic, credit card–style liability

¹⁴² Sorieul Interview, *supra* note 121.

¹⁴³ “It is estimated that 80 percent of electronic commerce transactions are business-to-business and likely to stay that way for many years.” Speech of Thomas Falk, Dir. of Industrial Policy, Fed. of Swedish Industries, OECD Ministerial Conference, *supra* note 81. Cf. Ragnar Nilsson, Dir. Karstadt AG, EuroCommerce, *It is the Issues, Not the Medium, that Define the Need for Regulation* (paper presented at the OECD Ministerial Conference, *supra* note 81) (“Business-to-consumer trade...will only account for 25% of the total electronic commerce world-wide” (referencing the European Information Technology Observer)) (on file with author).

¹⁴⁴ Based on these projections and Visa’s projection that global consumer electronic commerce will be as high as \$15.3 billion in 1998, the total global electronic commerce market may be as high as \$76.5 billion in 1998, broken down as follows:

TRANSACTION TYPE	PERCENTAGE OF TOTAL	DOLLAR VALUE
Business-to-business	80%	\$61.2 Billion
Consumer with credit cards	19.8%	\$15.1 Billion
Consumer w/o credit cards	0.2%	\$0.2 Billion
TOTAL	100%	\$76.5 Billion

979 regime on such a minuscule element of e-commerce transactions at this early stage in the
980 industry's lifecycle?¹⁴⁵

981

982 There are other fundamental differences between credit cards and certificates,
983 including that credit card processors obtain revenue on each transaction (generally
984 discounting transactions by 2 to 3 percent), thereby generating millions of dollars of
985 revenue annually that can pay for the \$50 limit on consumer liability. PKI certification
986 authorities, by contrast, generally receive no per-transaction revenues.¹⁴⁶ And yet, the
987 development and operational costs of a PKI are nontrivial, and "consumer and producer
988 costs for trustworthiness are difficult to assess."¹⁴⁷

989
990 In arguing for greater liability exposure for information providers, a few
991 commentators have claimed that the "[r]isk of fraud is not an element in the pricing of
992 wire transfers."¹⁴⁸ This is not the view of many industry participants. Norman Nelson,

See Jupiter Communications Online Intelligence, *Digital Commerce Strategies, Internet Payments: SET is Dead; SSL with Credit Cards Remains Standard Approach* (Sept. 4, 1998), available at <<http://www.jup.com/sps/commerce/briefs/9808/dc43/>>.

¹⁴⁵ In response to an argument for a consumer exemption for this very small percentage of non-credit card transactions, there is an argument that the small percentage of transactions coupled with the imposition of strict liability on CAs will provide a disincentive to make secure services available to consumers for such transactions. Many of these consumer transactions may not even involve payment – but instead simply are enjoying the benefits of secure messaging (encryption for confidentiality), without necessarily being subject to any bill or other Regulation E implications. So, if no money is involved, why should Reg. E-style rules apply?

¹⁴⁶ It has been argued that certification authorities could or should charge a transactional fee (in order to support higher insurance or reliance limits). However, the net effect of doing so may be to increase consumer cost, reduce consumer use and available services.

¹⁴⁷ TRUST IN CYBERSPACE, *supra* note 51, at Box 4.1.

¹⁴⁸ Letter from Jane K. Winn. & Paul Turner to Carlyle C. Ring, Jr. & Raymond Nimmer (Oct. 20, 1998) (copy on file with author) (regarding provisions in draft U.C.C. Art. 2B). The letter also asserts that "[n]o national interest is at stake in the drafting of Art. 2B in the way that the risks of bank or systemic failure resulting from a wire funds transfer was at stake in drafting Art. 4A." To the contrary, there are potential risks of "systemic paralysis" in PKI where systems cross-certify (the primary method urged to achieve interoperation in closed systems). *See generally* Kenneth A. Minihan, Dir., NSA, *Defending the Nation Against Cyber Attack: Information Assurance in the Global Environment*, 3 USIA ELECTRONIC J. (Nov. 1998), available at <<http://www.usia.gov/journals/itps/1198/ijpe/pj48min.htm>>. The National Research Council's *Trust in Cyberspace* reports that the:

993 CEO of CHIPS, has countered that “what it costs to cover fraud losses in wire transfers
994 will obviously be a function of [pricing].”¹⁴⁹

995

996 Furthermore, currently the greatest consumers of digital certificates are
997 companies wishing to facilitate authenticated, confidential communications with
998 customers via their commercial Web sites. Therefore, although consumers may rely on
999 server certificates to authenticate Web sites before providing credit card and order
1000 information, it is the commercial Web sites that are the primary “relying parties”—relying
1001 on the genuineness of consumers’ orders when providing goods and services.¹⁵⁰

1002

1003 **b. Certificate Status Checking by Relying Parties**

1004 Within the PKI business, technical, and legal communities, there is a general
1005 recognition that a potential relying party must check the revocation status¹⁵¹ of a

widespread interconnection of networked information systems allows outages and disruptions to spread from one system to others; it enables attacks to be waged anonymously and from a safe distance; and it compounds the difficulty of understanding and controlling these systems. Apart from the obvious dangers of the increased complexity, the interconnections themselves create new weak points and interdependencies. Problems could grow beyond the annoyance level that characterizes infrastructure outages today, and the possibility of catastrophic incidents is growing.

TRUST IN CYBERSPACE, *supra* note 51, at 15.

¹⁴⁹ Telephone Interview of Norman Nelson by Michael S. Baum (Nov. 24, 1998) (on file with author). The celebrated case of *Evra Corp. v. Swiss Bank Corp* succinctly recognized that the

success of the wholesale wire transfer industry has largely been based on its ability to effect payment at low cost and great speed. Both of these essential aspects of the modern wire transfer system would be adversely affected by a rule that imposed on banks liability for consequential damages. A banking industry amicus brief in *Evra* stated: "Whether banks can continue to make EFT services available on a widespread basis, by charging reasonable rates, depends on whether they can do so without incurring unlimited consequential risks. Certainly, no bank would handle for \$3.25 a transaction entailing potential liability in the millions of dollars.

673 F.2d 951 (7th Cir. 1982); *see* U.C.C. § 4A-305 cmt. 2.

¹⁵⁰ “Client certificates” that are used to authenticate consumers on the Web are not yet widely deployed.

¹⁵¹ Depending upon the implementation and governing rules, this obligation is typically satisfied by checking the then-current certificate revocation list (CRL) or an on-line certificate status service (such as implementing the PKIX Working Group, Internet Engineering Task Force, X.509 Internet Public Key Infrastructure Certificate Status Protocol-OCSP) (Sept. 98), *available at* <<http://search.ietf.org/internet-drafts/draft-ietf-pkix-ocsp-07.txt>>.

1006 certificate before he or she may justifiably rely on it (or seek damages against the
1007 certification authority or subscriber).¹⁵² Checking the status of a certificate is becoming at
1008 least a *usage of trade*, if indeed it is not already an affirmative obligation. Under well-
1009 understood PKI theory, status checking is a critical procedure and precondition for use of
1010 certificates and thus will invariably be observed regularly. It is consistent with the
1011 traditional legal principle which tries to apportion legal responsibility among innocent
1012 parties to reflect which were in a position to avoid risk to all the parties. The *Digital*
1013 *Signature Guidelines*¹⁵³ and other guidelines, practices,¹⁵⁴ and rules expressly advance

¹⁵² Indeed, revocation checking is one of the most widely recognized usages of trade in global PKI. Additionally, “other computer-based means,” such as credit card payment systems, obligate the relying party (e.g., a merchant-vendor) to have a customer’s credit card transaction authorized by the card issuer as a precondition of assured payment. *See* VISA INTERNATIONAL BYLAWS AND OPERATING RULES, § 6.13 (1998). Also, electronic funds transfer (EFT) via automated teller machines (ATMs) exemplifies a mechanism that by necessity obligates the relying party (payee bank) to obtain authorization of a customer’s credit limit/status before completing a transaction for assured payment from the payor bank. One exception to this rule could be for *transactional certificates*. *See* DIGITAL SIGNATURE GUIDELINES, *supra* note 20, § 1.34.

¹⁵³ The *Digital Signature Guidelines* state that reliance on a certificate after notice of revocation published in a CA’s repository is unreasonable, and relying parties assume the risk of forgery or repudiation. *See* DIGITAL SIGNATURE GUIDELINES, *supra* note 20, §§ 1.26, 1.26.1-1.26.2 (publication in repository can serve as notice), 3.12, 3.12.2, 5.4.2 (relying on a revoked certificate after notice of revocation is likely to be considered unreasonable reliance), §§ 5.3(2), 5.3.2 (relying party unreasonably relying on a certificate assumes risk that signature is forged or unattributable to signer). In light of such adoption, a court should find certificate status checking to be a regularly observed practice, and thus a usage of trade.

¹⁵⁴ This obligation is also implicated by the IETF’s Public Key Infrastructure (PKIX) Working Group’s influential Certificate Policy and Certification Practices Framework, also known as “PKIX Part 4.” *See* Santosh Chokhani & Warwick Ford, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* § 4.2.1 (last modified Apr. 25, 1998), available at <<http://search.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt>>. PKIX Part 4 has become the industry-standard framework for writing certification practice statements and certificate policy definitions in the PKI industry. Consequently, certificate policy definitions developed by high-profile entities such as the ANX, the Government of Canada, and the National Automated Clearing House Association’s Authentication and Network of Trust Pilot Program follow the PKIX Part 4 framework and, in keeping with it, have imposed an obligation to check certificate status. *See* Automotive Industry Action Group, *Automotive Network eXchange® (ANX®) Certificate Policy* § 2.1.5 (unpublished document, on file with author); Government of Canada PKI Policy Management Authority, *Certificate Policies for the Government of Canada Public Key Infrastructure* §§ 2.1.4.3, 4.4.10 (V2.0, last modified Aug. 1998), available at

1014 this obligation, and PKI liability regimes are greatly dependent on it.¹⁵⁵ This is one of the
1015 most fundamental and important precepts for many PKIs. In fact, it was not addressed in
1016 UNCITRAL's draft model rules on electronic signatures until the most recent *Note from*
1017 *the Secretariat* – and even then, it was not expressed as an affirmative obligation.

1018

1019 A person is entitled to rely on an enhanced electronic signature, provided it
1020 takes reasonable steps to determine whether the enhanced electronic
1021 signature is valid and has not been compromised or revoked.¹⁵⁶

1022

1023 This issue is so essential for PKI within a broad range of applications that its
1024 absence would hamper if not significantly impede the development of important
1025 segments of the industry.

1026

<<http://www.tiac.net/biz/bcslegal/cp/CPaugWord2x.doc>> (providing revocation checking requirement for all classes of certificates except for Rudimentary Assurance), The Internet Council, National Automated Clearing House Association, *Authentication and Network of Trust Pilot Program Certificate Policy* § 4.2.1.5.3 (unpublished document, on file with author).

Most CAs require relying parties to check certificate status before reliance. *See, e.g.,* BelSign, BelSign, NV/SA, *BelSign_Certification Practice Statement* § 8.1 (last modified May 1997), available at <<http://www.besign.be/en/repository/CPS.txt>>; CertiSign, *Declaração das Práticas de Certificação da CertiSign* (version 1.0) (visited Oct. 10, 1998), available at <<http://www.certisign.com.br/info/CertiSignCAPolicy.html>>; British Telecommunications plc, *BT Certification Practice Statement* § 8.1 (last modified July 10, 1998), available at <<http://www.trustwise.com/repository/index.html>>. GTE Internetworking states that parties relying on its SureServer Certificates “are advised” to determine whether a SureServer Certificate has expired or been revoked, and *VeriSign Certification Practice Statement* § 8.1 (last modified May 15, 1997), available at <<https://www.verisign.com/repository/CPS1.2/CPSCH8.HTM>>. GTE Internetworking Inc., *Certificate Practice Statement for CyberTrust SureServerSM Certificates Version 1.0* § 1.8 (last modified Aug. 3, 1998), available at <<http://www.bbn.com/products/security/cytrust/cps.htm>>.

¹⁵⁵ PKI commercial risk management programs particularly CA obligations to insurers and reinsurers are dependent upon recognition of this fundamental obligation. Note, there are some applications that use certificates that may not require certificate status checking (such as certain SET implementations that use pre-existing bankcard authorization mechanisms). In such cases, user agreements can waive or otherwise make certificate status checking optional.

¹⁵⁶ UNCITRAL Draft ARTICLES, *supra* note 67, Art. G. (Reliance on an enhanced electronic signatures).

1027 **c. Presumptions**

1028 Legal presumptions¹⁵⁷ are used to simplify and clarify legal processes. More
1029 important for commerce and trade, however, is that they provide the basis for allocating
1030 risk and pricing products. The great bulk of commercial transactions do not involve legal
1031 processes, and the business community is more concerned with its ability to set prices
1032 and allocate risk than with the legal implications of presumptions, regardless of the
1033 importance of those implications to legal commentators. Some proponents of avoiding
1034 presumptions at this point state that if they are adopted too early in the development of
1035 market practices, it may alter the market. Others are concerned about consumer rather
1036 than business interests and have not found a way to resolve them.

1037 Some form of presumptions should be considered, however, either “strong” or
1038 “weak,” to bolster the legal effect of trustworthy digital signatures, *at least in a second*
1039 *or later phase of rule making*.¹⁵⁸ Presumptions have been widely used in certain
1040 historically significant areas related to e-commerce, such as for electronic funds transfer
1041 (EFT), and can be used to advance secure e-commerce.¹⁵⁹ Presumptions concerning secure
1042 e-commerce are currently a subject of spirited debate within rule-making bodies.¹⁶⁰ The

¹⁵⁷ A rule of law by which finding of a basic fact gives rise to existence of presumed fact, until presumption is rebutted. “*Presumption*,” BLACKS LAW DICTIONARY 617 (abridged 5th Ed. 1983).

¹⁵⁸ The suggestion of waiting until a “second or later phase of rulemaking” is a practical consideration – so as not to prevent progress from being made on other important provisions because of controversy concerning presumptions.

¹⁵⁹ Such as under the U.C.C. Art. 4A, and the UNCITRAL Model Law on International Credit Transfers, REPORT OF THE UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW ON THE WORK OF ITS TWENTY-FIFTH SESSION, U.N. GAOR, 47th Sess. Supp. No. 17, Annex 1, U.N. Doc. A/47/17 (1992).

In the context of EFT, when a party instructs its bank to transfer funds, the transaction can be undertaken with considerable finality based on presumptions and liability limitations. Such finality is an inducement, if not a compelling necessity, for the financial institution to act.

Additionally, South Carolina and Singapore have adopted the secure signature concept (which contains presumptions), and Canada has proposed legislation to do the same, *see* Bill C-54 (1998), *available at* <http://www.parl.gc.ca/36/1/parlbus/chambus/house/bills/government/C-54/C-54_1/C-54TOCE.html>. Iowa and Pennsylvania have also considered this concept.

The *UNCITRAL Model Law* contains many instances where certain facts are “presumed” or “deemed.” *See, e.g.*, UNCITRAL MODEL LAW, *supra* note 115, §§ 13(2) (attribution of a data message as between originator and addressee), 14(6) (acknowledgement of satisfaction of technical standards), 14(5) (presumption or receipt upon originators receipt of acknowledgement).

¹⁶⁰ *See* UNCITRAL Draft Uniform Rules, *supra* note 117, Note by the Secretariat (recounting the difficulty in resolving the presumptions issue); *see* Ben Beard, *Memorandum to the Unif. Elec.*

1043 debate has focused largely on the effectiveness and fairness of presumptions regarding
1044 the *attribution* of enhanced or secure electronic signatures. Without harboring any
1045 illusion that all presumption issues may be generally resolved in the short term, there
1046 may be a realistic shorter-term solution—to enact *at least* “weak” self-authentication
1047 rules that would cover the integrity and correctness of the technology but not necessarily
1048 attribution of identity.¹⁶¹

1049 Critics contend that weak presumptions are ineffective, since they “burst” and
1050 disappear immediately upon being challenged. Nonetheless, certain presumptions can be
1051 useful, even if only weak in effect, such as an evidentiary presumption making enhanced
1052 or secure digital signatures *self-authenticating*. The U.S. Department of the Treasury has
1053 proposed such a rule, urging that:

1054

1055 There are several reasons that support the insertion of a limited self-
1056 authentication clause If public-key encryption has been properly
1057 implemented, the risk of a successful forgery or alteration of a digital signature is
1058 extremely remote, and is significantly less than the risk of forgery or alteration
1059 for paper records. Furthermore, although a legal showing of authenticity in the
1060 absence of a self-authentication provision almost certainly could be
1061 accomplished, such a showing would require considerable time and resources.
1062 Among other things, it would entail extensive scientific testimony on encryption,
1063 leading to an expensive and unproductive “battle of the experts.” Use of a self-
1064 authentication provision would avoid this wasteful problem. . . .

1065 In almost all cases, the existence of a digital signature should be beyond
1066 reasonable dispute. The most likely challenges to a digital signature and an
1067 electronic record to which it is affixed will turn not on whether a digital signature
1068 exists, but on whether it should be attributed to a particular person.¹⁶²

1069

1070 Another example is Rule 902 of the Federal Rules of Evidence (and parallel state
1071 rules) which declares many types of documents—including many that are arguably less

Trans. Act Drafting Committee and Observers (Sept. 18, 1998) (summarizing arguments for and against presumptions), available at <<http://www.law.upenn.edu/library/ulc/uecicta/eta1098m.htm>>.

¹⁶¹ This is not the author’s favored position, but it might end the current stalemate and successfully advance the development of viable rules. The notion of including self-authentication presumptions associated with trustworthy digital signatures was proposed by the author in Michael S. Baum, *Linking Security and the Law of Electronic Commerce*, pt. 4 (1992) available at <http://www.verisign.com/respository/pubs/linking_security>.

¹⁶² Proposed Regulations Governing Agencies for the Issue and Offering of United States Savings Bonds, Including Sales by Electronic Means, 63 Fed. Reg. 23695, 23699 (Apr. 30, 1998).

1072 trustworthy than are certain digital signatures—to be self authenticating.¹⁶³

1073

1074 Concerns about the potential harmful effect of presumptions on consumers can be
1075 mitigated by ensuring that presumptions are invoked only under specified conditions¹⁶⁴
1076 and are, for the time being, kept weak. As discussed above, since most consumer
1077 transactions are executed via credit card, consumer exposure is limited notwithstanding
1078 certain presumptions. And, if coupled with the increasing availability of technical and
1079 legal mechanisms to protect against the potential risks of PKI,¹⁶⁵ then presumptions can
1080 generally benefit the e-commerce community. It is important to recognize, as well, that
1081 consumers can be the primary beneficiaries of some presumptions – such as where the
1082 presumption induces a vendor to act on a computer-based order for goods or services or
1083 to make new services available (or available more inexpensively) to consumers.

1084

1085 The benefits of PKI include greater transactional certainty for Internet commerce
1086 than can be obtained using “alternative” technologies. That certainty arises, in part, from
1087 the enhanced and unique security services provided by PKI, which in turn are a function
1088 of the greater resources expended to enable it. And all other things being equal, parties
1089 that take reasonable efforts to secure their transactions should enjoy a better position
1090 legally than do those who do not. The use of presumptions commensurate with a
1091 reasonable level of effort expended to protect one’s transactions is appropriate and, from
1092 a social policy perspective, provides an important incentive to all participants.

¹⁶³ See FED. R. EVID. Rule 902 (Self-Authentication). Rule 902 provides that “extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to: domestic public documents under seal, domestic public documents not under seal, foreign public documents, certified copies of public records, official publications, newspapers and periodicals, trade inscriptions and the like, acknowledged documents, commercial paper and related documents, presumptions under acts of congress.”

It has also been argued that a self-authentication provision is unnecessary outside of Common Law jurisdictions and therefore should not be included in the *UNCITRAL Model Law* or other international model rules. This is unpersuasive since there are many instances in the *UNCITRAL Model Law* (and other rules) where special accommodation has been made to resolve problems within specific legal systems, such as to declare electronic records to be no less effective than “originals” (to address common law barriers to electronic commerce). See *UNCITRAL MODEL LAW*, *supra* note 115, Art. 8.

¹⁶⁴ Such as where a “qualified” security procedure is invoked, where its use is commercially reasonable, where it is implemented in a trustworthy fashion, and is relied upon reasonably and in good faith. See the Illinois Electronic Commerce Security Act, § 10-110 cmt. 3. Also, the self-authentication presumptions in Fed. R. Evid. Rule 902 apply no less to consumers than to others.

¹⁶⁵ See *supra* note, 137-40 and corresponding text.

1093

1094

SUMMARY

1095

1096 The development of a global PKI infrastructure is real and dramatically
1097 accelerating. There is little doubt that PKI architecture is being embedded throughout the
1098 information infrastructure worldwide as well as in diverse individual applications.
1099 Simply put, PKI is critical and well suited to ensuring a sustainable, secure e-commerce
1100 environment. Because e-commerce technology and the technologies and legal structures
1101 that support it are becoming ever more complex, threats to the viability of secure global
1102 e-commerce will increase in the absence of a robust, implemented global PKI. Therefore,
1103 rules to specifically facilitate and ensure greater certainty for PKI are important.
1104 Technology-neutral rules, no matter how well intentioned, will fail in this regard. The
1105 need for a global secure infrastructure well outweighs the risk, suggested by some, that
1106 PKI rules could become outdated or restrictive.

1107

1108 Does this mean that we necessarily embrace any current or proposed PKI
1109 regulation? No, because despite admirable initiatives to date, PKI rules are generally not
1110 ready for prime time. Nonetheless, inaction is not the best option. We need to proactively
1111 advance the develop of viable PKI rules proposals that accommodate, flexibly, diverse
1112 business models. If we do not do so, governments will invariably regulate without our
1113 meaningful participation-- and that is simply unacceptable.

1114

1115

**

1116

1117 *Final note:* The author is preparing a new document, entitled “Proposed Issues
1118 for a Model Law on PKI” that will detail the issues he believes should be included in the
1119 UNCITRAL Model Law on PKI. That document will be available at:
1120 <www.verisign.com/repository/pubs/uncitral_pki_proposal>.