1996

The Essential Role of Trusted Third Parties in Electronic Commerce

A. Michael Froomkin
University of Miami School of Law, froomkin@law.miami.edu

A. MICHAEL FROOMKIN*

The Essential Role of Trusted Third Parties in Electronic Commerce

BY now it is well known that the Internet is a global, but insecure, network.[1] It is also increasingly well understood that cryptography[2] can contribute greatly to the ransactional security that Internet commerce so obviously lacks.[3] What is less well understood is that cryptography is only part of the security story. Many cryptographic protocols for secure electronic transactions require at least one trusted third party to the transaction, such as a bank or a "certification authority" (CA). These partly cryptographic, partly social, protocols require new entities, or new relationships with existing entities, but the duties and liabilities of those entities are uncertain. Until these uncertainties are resolved, they risk inhibiting the spread of the most interesting forms of electronic commerce and causing unnecessary litigation.

This Article aims to describe what CAs do, explain why they

 Associate Professor, University of Miami School of Law; B.A., 1982, Yale College; M.Phil., 1984, Cambridge University; J.D., 1987, Yale Law School. Internet: froomkin@law.miami.edu. Tom Baker, Caroline Bradley, Patrick Gudridge, Trotter Hardy, Richard Hausler, Francis Hill, Mark Lemley, Jessica Litman, Charles Merrill, Daniel Murray, and Katie Sowle provided helpful comments on earlier drafts of this paper. I am also grateful to Alan Asay, Bob Jueneman, Chuck Miller, and many other past and present members of the ABA Information Security Committee for helpful discussions of many technical questions; Richard Field, Hal Finney, and Lucky Green for sharing their expertise regarding electronic cash and related matters; Ann Klienfelter, Claire Donnelly, SueAnn Campbell and Nora de la Garza for reference and information retrieval help; Rosalia Lliraldi for secretarial assistance; and Erica Wright for research assistance. I am particularly grateful to Keith Aoki, Richard Painter, and the University of Oregon School of Law for inviting me to participate in this Conference on Innovation and the Information Environment. Unless otherwise noted, this Article attempts to reflect legal and technical developments up to February 1, 1996.

[1] The FBI estimates that eighty percent of computer crime it investigates involves the Internet. DAVID ICOVE ET AL., COMPUTER CRIME: A CRIMEFIGHTER'S HANDBOOK 129 (1995).

[2] For an explanation of cryptographic techniques see *infra* Part I.A-C.

[3] *See generally* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

are important to electronic commerce, and suggest that they are likely to provoke some interesting legal problems. It does not attempt to describe a complete legal regime for the regulation of CAs in electronic commerce.[4] The coming wave of faceless electronic commerce presents a number of challenges; opportunities for fraud and error and for the prevention of fraud and error are interwoven with the solutions to these difficulties. Although accounts of fraud in commercial electronic transactions (as opposed to simple theft of data or services by a stranger) on the Internet remain very rare, this may reflect the low level of Internet commerce today more than any virtues of the medium.[5]

Utah was the first state to attempt to provide a regulatory framework for CAs. The Utah Digital Signature Act provides for a safe harbor against most liability for those who qualify.[6] No one has qualified to date,[7] and the Act does not define the duties and liabilities of those who do not qualify for the safe harbor.[8] Clarification of the duties and liabilities of CAs in the absence of legislation should thus serve the interests of all parties to an electronic transaction in which a certificate plays a role. Other states, and perhaps some day the United States Congress, will eventually have to decide whether to enact digital signature laws of

---

[4] Attempts to do this are in progress. The state of Utah passed a Digital Signature Act in 1995, UTAH CODE ANN. tit. 46, ch. 3 (1995), and amended it in 1996. Digital Signature Act Amendments, 52nd Leg., Gen. Sess., 1996 Utah Laws 188 (LEXIS, Codes library, UTCODE file) (to be codified at UTAH CODE ANN. tit. 46, ch. 3) (hereinafter all cites to the UTAH CODE ANN. incorporate the 1996 amendments). As of November 1995, no certification authorities had qualified under the Utah Act. *See* Introductory Commentary, History and Current Status of the Utah Act *1, *available online* URL http://www.state.ut.us/ccjj/digsig/dsut-int.htm. The Information Security Committee of the Section on Science and Technology of the American Bar Association issued the Draft Digital Signature Guidelines for public comment which ended in January 1996. Draft Digital Signature Guidelines, *available online* URL http://www.state.ut.us/ccjj/digsig/dsut-gl.htm [hereinafter Draft Guidelines]. The Guidelines are currently being revised. The state of California has passed a statute delegating to the Secretary of State powers to make rules regulating the use and verification of digital signatures. *See* 1995 Cal. Legis. Serv. Ch. 594 (A.B. 1577) (West). On March 29, 1996, Washington State approved a digital signatures statute with an effective date of January 1, 1998. *See* Washington Electronic Authentication Act, 1996 Wash. Legis. Serv. Ch. 250 (S.B. 6423) (WL, WA LEGIS Library).

[5] "The Net currently is a universe of browsers rather than shoppers." Larry Marion, *Who's Guarding the Till at the CyberMall?*, DATAMATION, Feb. 15, 1995, at 38, 41.

[6] UTAH CODE ANN. § 46-3-309 (1996).

[7] Introductory Commentary, History and Current Status of the Utah Act, *supra* note 4, at *1.

[8] UTAH CODE ANN. § 46-3-201(5).

their own, and they may find it helpful to have a better understanding of the legal background against which a comprehensive legislative program may be drawn.

Before embarking on a discussion of the role of trusted third parties in electronic commerce, it is useful to review basic cryptographic techniques such as public-key cryptography and digital signatures. Cryptographically sophisticated readers should skip to Part I.D., which begins a description of certification authorities and discusses the various types of digital certificates they may issue, or to Part II, where the discussion of the application of these techniques to Internet commerce begins. In order to show just how hard it can be to determine what legal rules apply to this new world of electronic commerce, Part III offers an introductory discussion of the liability of a CA that issues an erroneous certificate.

I

CRYPTOGRAPHIC KEYS, DIGITAL SIGNATURES, DIGITAL CERTIFICATES, AND THE PEOPLE WHO ISSUE THEM

A. Public-Key Cryptography

A *public-key cryptosystem* is one in which messages encrypted with one key can only be decrypted with a second key, and vice-versa. A strong public-key system is one in which possession of both the algorithm and one key gives no useful information about the other key and thus no clues as to how to decrypt the message.[9] The system gets its name from the idea that the user will publish one key, but keep the other one secret. The world can use the public key to send messages that only the private key owner can read; the private key can be used to send messages that could only have been sent by the key owner.

With the aid of public-key cryptography it is possible to establish a secure line of communication with anyone who is using a compatible decryption program or other device. Sender and receiver no longer need a secure way to agree on a shared key. If Alice wishes to communicate with Bob, a stranger with whom

[9] *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C 470-74, 501-02 (1996) (stating that security of public-key systems depends on inability of factoring large numbers rapidly or on the continuing inability of mathematicians to solve the long-standing problem of calculating discrete logarithms).

she has never communicated before, Alice and Bob can exchange the plain text of their public keys. Then, Alice and Bob can each encrypt their outgoing messages with the other's public key and decrypt their received messages with their own secret, private key. The security of the system evaporates if either party's private key is compromised, that is, transmitted to anyone else.

Thus, if Alice wants to send a secure e-mail message to Bob, and they both use compatible public-key cryptographic software, Alice and Bob can exchange public keys on an insecure line. If Alice has Bob's public key *and knows that it is really Bob's* then Alice can use it to ensure that only Bob, and no one pretending to be Bob, can decode the message.

The problem facing Alice in this scenario, however, is that there is no more reason to trust an e-mail message purporting to be from Bob that says "here is my public key" than there is to trust any other e-mail message purporting to be from Bob. Lacking independent confirmation, Alice has no way of knowing whether the message is really from Bob or from an imposter. (Bob has the same problem regarding Alice.) One bit looks exactly like another, making it possible for Mallet to forge messages purporting to come from either Alice, Bob, or both.[10] And, if Mallet is able to masquerade as Bob in an e-mail message, Mallet can just as easily send Alice his own public key, claiming that it belongs to Bob. Without help from a source external to the Internet communication, either a trusted third party or some "out-of-band" (non-Internet) communication that is reliable, Alice has no way of assuring herself of the authenticity of any e-mailed communication from a stranger, regardless of what it says. Alice needs some assurance to feel confident that she is not sending the details of a tender or her financial details to a malicious stranger who might seek to profit from it at her expense. Of course, if the message is from someone Alice already knows, the message itself may provide internal clues of its authenticity—for example, the clichéd scenario in war movies in which soldiers radio from behind enemy lines and identify themselves by telling their buddies about a well-remembered poker hand.

A third-party registry of public keys does not really solve Alice's and Bob's problem unless the registry also certifies the accu-

[10] This is the classic "man-in-the-middle" attack. *Id.* at 48-49.

racy of the information it contains. Suppose that Carol runs an Internet directory service that contains names, e-mail addresses, and public keys. Being a generous person, Carol invites anyone to sign up for free, and makes no effort to check the data submitted to her. Alice has no way of knowing whether the entry for Bob was sent in by Bob, or whether it was sent in by Mallet claiming to be Bob. If Mallet sent it in, he will have an entry with Bob's name, Mallet's e-mail address, and Mallet's public key. A directory service alone is thus of little value in providing the assurance as to Bob's identity that Alice wants.[11]

The World Wide Web (Web) introduces some complications into this picture but does not alter the basic substance. Although at this writing it is very difficult for Alice to completely mask the identity of the account accessing a Web page, prototype anonymous Web browsers are currently being developed.[12] Even if Alice does not have access to an anonymous browser, there is no way for Bob to know whether Alice is using an account that can be traced to her, or an account procured under a pseudonym, or a hacked account belonging to someone else entirely. Similarly, in the ordinary course, Bob's Web address identifies his Web page as residing on a particular machine whose physical location can be deduced from information readily available on the Internet,[13] although the address itself is less informative than a telephone number.[14] However, some services sell anonymous Web pages[15] and Web addresses can be hacked; furthermore, messages to and from a Web server also are at least theoretically subject to a "man in the middle" attack by which message packets are intercepted and replaced with the attacker's messages.[16]

---

[11] One method of addressing this problem is the "web-of-trust" approach. *See infra* note 26.

[12] Prototype anonymous Web proxies are in development. *See, e.g.*, Anonymizer FAQ, *available online* URL http://anonymizer.cs.cmu.edu:8080/faq.html.

[13] For a more detailed description of these mechanisms see BRENDAN P. KEHOE, ZEN AND THE ART OF INTERNET (1992), *available online* URL http://www.cs.indiana.edu/docproject/zen/zen-1.0_3.html.

[14] For example, the organization that created www.trilateral.com is (almost certainly) not the real Trilateral Commission. *See* The Trilateral Commission, *available online* URL http://www.trilateral.com (including humorous cites and links to "other conspiracies").

[15] *See, e.g.*, Community ConneXion, The Internet Privacy Provider, *available online* URL http://www.c2.org/web.phtml.

[16] *See* SCHNEIER, *supra* note 9, at 48-49.

B. Digital Signatures

Public-key systems also allow users to append a *digital signature* to an unencrypted message. A digital signature encrypted with a private key uniquely identifies the sender and connects the sender to the exact message. When combined with a digital time stamp[17] the message can also be proved to have been sent at a certain time. Anyone who has the user's public key can then *verify*[18] the integrity of the signature. Because the signature uses the original text as an input to the encryption algorithm, if the message is altered in even the slightest way, the signature will not decrypt properly, showing that the message was altered in transit or that the signature was forged by copying it from a different message.[19] A digital signature copied from one message has an infinitesimal chance of successfully authenticating any other message.[20]

Again, however, the utility of a digital signature as an authenticating tool is limited by the ability of the recipient to ensure the authenticity of the key used to verify the signature. If Alice uses her private key to sign an otherwise unencrypted message, Bob can verify that Alice really sent it only if Bob knows Alice's public key.[21] In order to rely on the authenticity of that public key,

---

[17] *See infra* Part I.D.4.

[18] The Utah Digital Signature Law states that:

> "Verify a digital signature" means, in relation to a given digital signature, message, and public key, to determine accurately that:
> (a) the digital signature was created by the private key corresponding to the public key; and
> (b) the message has not been altered since its digital signature was created.

UTAH CODE ANN. § 46-3-103(40).

[19] Digital signatures achieve this by computing a *hash value* of the message and then encrypting the hash value with the user's private key. *See infra* text following note 59 (describing hash functions). The recipient checks the digital signature by decrypting the hash value with the sender's public key, then comparing the hash value with the hash value of the file received. If the two numbers are the same, the file is authentic and unchanged. *See* Paul Fahn, RSA Laboratories, Answers to Frequently Asked Questions About Today's Cryptography § 2.13 (1993), *available online* URL http://www.rsa.com/pub/faq/faq.asc.

[20] *See* SCHNEIER, *supra* note 9, at 38 (noting that a digital signature using a 160-bit hash has only a one in 2^{160} chance of misidentification).

[21] Even if Bob does not know that the public key belongs to Alice, the key may have value in identifying a series of messages as emanating from a single source calling itself "Alice." This property is particularly valuable in establishing the continuity of a pseudonym in public forums, in preventing "nym collision" (in which two or more parties accidentally use the same pseudonym), or "nym hijacking" (in which Mallet sends messages signed "Alice" in order to free ride on the good reputation "Alice" has accumulated among those familiar with her messages). *See* A. Michael

however, Bob needs to get it from some source other than the "Alice" sending the message, because if Mallet is forging a message from Alice he will send his own public key as well, claiming that it actually belongs to Alice. Since Mallet has the private key corresponding to the public key he sends Bob, Bob's attempt to verify the signature of the forged message will result in a confirmation of the message's authenticity—even though it is not really from Alice at all. In contrast, if Bob has access to Alice's real public key from some outside source, and uses it to verify the message signed with Mallet's private key, the verification will fail, revealing the forgery.

In short, if Alice and Bob are strangers with no alternate means of communication then no digital signatures, indeed no amount of cryptography standing alone, will reliably authenticate or identify them to each other without the assistance of some outside source to provide a link between their identities and their public keys. Any outside source that reasonably inspires trust will suffice: for example, the telephone company might include its public key in the monthly phone bill, or corporations might publish their public keys in the newspaper. Or, the outside source could be a trusted third party such as a mutual friend, a government agency, or a business that offers on-line verification services.

C. Certification Authorities

A *Certification Authority* (CA) is a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing digital *certificates* that attest to some fact about the subject of the certificate.[22]

In order for either Bob or Alice to be willing to accept certificates issued by Carol, a CA, Bob and Alice must have confidence that Carol's public key is really Carol's and not another manifestation of the wily Mallet. One way to achieve this confidence is

---

Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 PITT. J.L. & COMMERCE (forthcoming 1996).

[22] *See generally* WARWICK FORD, COMPUTER COMMUNICATIONS SECURITY: PRINCIPLES, STANDARD PROTOCOLS AND TECHNIQUES 93-101 (1994). The International Telecommunications Union defines a CA as a body "trusted by one or more users to create and assign certificates." MICHAEL S. BAUM, U.S. DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY: LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES 5 (1994) (quoting ITU-T, X.509 § 3.3 (1993)).

to have an identifying certificate from Trent, another CA, certifying Carol's key. CAs that certify other CAs are said to participate in a *certificate chain*, with a *root certificate* at the bottom of the tree.[23] Unfortunately, this just shifts the problem to the validity of Trent's CA's public key.

One solution to this problem contemplates a governmental role in certifying the keys of CAs. The root key would belong to a state or federal agency, and the few CAs that met state licensing requirements would be rewarded with government certification of their root key.[24] These CAs would then certify the root keys of organizations that wished to manage their own certificates. A CA might certify the root key of ABC Corp, which would in turn be used to certify the keys of, for example, the key manager in each corporate division, which in turn would certify the keys of salespeople, purchasing agents and press secretaries.

The more levels there are in a certification tree, the more certificates Alice needs to check to ensure that Bob's certificate remains valid. Suppose that Bob's digital signature is supported by a certificate issued by CA1, which has a public key certified by CA2, in turn certified by CA3, which in turn is certified by a state government. If the state government issues a notice of revocation for the certificate of CA3 because, for example, someone has broken its private key, all certificates descending from CA3 are now suspect. If CA3 could say with certainty that its key remained safe until a particular date, then certificates bearing a secure timestamp showing that they were issued before that time would still be reliable.[25] Alice can work all this out, but it takes some computing time, and it may require accessing as many different databases as there are CAs which also could be costly or time-consuming.[26]

---

[23] Warwick Ford, *Advances in Public-Key Certificate Standards*, SIG SECURITY, AUDIT & CONTROL REV., July 1995, at 9, 10.

[24] *See, e.g.*, UTAH CODE ANN. §§ 46-3-104, 46-3-201.

[25] The time stamp from an outside source is essential. Alice cannot trust a certificate from CA3 that *claims* to have been issued during the safe period because the party forging the certificate could be lying about the time as well. A certificate with an outside timestamp proving that it was issued before CA3's key was compromised can be revalidated by a new, trustworthy certificate from CA3 or any other CA, thereby extending its lifespan considerably. *See* Dave Bayer et al., *Improving the Efficiency and Reliability of Digital Time-Stamping*, *in* SEQUENCES II: METHODS IN COMMUNICATION, SECURITY, AND COMPUTER SCIENCE 329, 332-33 (Renato Capocelli et al. eds., 1993).

[26] Certification authorities are not the only means by which strangers can be persuaded to trust each other. An alternate system, called the web-of-trust, blurs the

The few CAs currently in operation have dealt with the absence of an agreed root certification authority by simply signing their own keys and posting the self-certified key on their Web sites.[27] The self-certified key is then mirrored on other computers.[28] This self-certification, in which the CA relies on its reputation gleaned from other business dealings, fits a model of relatively flat certification hierarchies, in which users turn to CAs, be they suppliers or the United States Postal Service, that they already know in other contexts. One expert predicts that

---

distinction between CAs and users. Every participant in a web-of-trust system is able to issue notices about whom they know and trust, and there is no central authority. In this system, Carol may provide a directory of e-mail addresses and public keys (the *key server*), but if so, she makes no representations at all as to their ownership or authenticity. Users then provide authenticating statements for each other. Typically this is done by meeting face-to-face and showing identification, and then by exchanging public keys signed with their private keys. Alternately, users can exchange "key fingerprints"—a short form of the key that points to the key's location on the key server. If Alice wishes to make it easy for people she has not met to contact her securely, Alice must upload these authentications to the key server. If Alice has her key signed by David, whom Bob knows or trusts, Bob can safely assume that the signature purporting to be from "Alice" is not in fact an impostor's. Suppose, however, that Alice and Bob do not have any friends in common, but that Bob's friend David has signed Ted's key, and Ted has signed Alice's key. From Bob's point of view this is not as good as if David, whom he knows, had signed Alice's key, but it is considerably better than nothing. Bob needs to decide how many intermediaries he is willing to accept before he considers a public key to be unreliable. The increase in the length of the chain of authentication can be offset by finding multiple routes to Alice. For example, Bob may still feel reasonably secure if he can establish three relatively long but independent chains of authentication. *See* Philip Zimmermann, PGP™ User's Guide Volume I: Essential Topics (Oct. 11, 1994), *available online* URL ftp://net-dist.mit.edu/pub/PGP. This web-of-trust approach is the foundation of the PGP encryption system.

The web-of-trust model has the advantage of being independent of any central authority. It has the disadvantage that it requires Alice either to trust strangers when she has no friends in common with Bob or to accept that there are large numbers of people with whom she cannot securely communicate. In contrast, the CA model is designed to make it possible for all strangers to communicate regardless of whether they have any friends in common, and to define with some precision the degree of trust that they can put in the CA's representations about strangers. This Article discusses CA-based systems, but this is not intended to denigrate the utility of a web-of-trust system. If it is true that all people are within six degrees of separation from each other, the web-of-trust may be a valuable system.

[27] *See, e.g.*, The Sun CA's Certificate, *available online* URL http://www.incog.com/self.html; Internet PCA Registration Authority Root Key Information, *available online* URL http://bs.mit.edu:8001/ipra.html; Netscape Test Certification Authority, *available online* URL http://home.netscape.com/newsref/ref/netscape-test-ca.html.

[28] Mirroring makes Mallet's job more difficult; however, if Mallet is able to filter all messages from Alice's computer to the rest of the world, no amount of mirroring will defeat him.

the wave of the future will be relatively flat hierarchies, in which organizations have a root certificate for internal purposes that is certified by at most one other CA.[29] It is simply too early to know which certification model will predominate, but it is interesting to consider that today the major indicator of the authenticity of most accountant's and lawyer's opinions provided to third parties is the letterhead (easily forged) and the representation of authenticity by the party proffering the opinion.

D. Certificates

A *certificate* is a digitally signed statement by a CA that provides independent confirmation of an attribute claimed by a person proffering a digital signature. More formally, a certificate is a computer-based record which: (1) identifies the CA issuing it, (2) names, identifies, or describes an attribute of the subscriber, (3) contains the subscriber's public key, and (4) is digitally signed by the CA issuing it.[30]

As a formal matter, a certificate binding a fact to a public key does not need to have a description of the level of inquiry used to confirm the fact. Bob would be foolish, however, to trust a certificate that made no representation, if only through incorporation by reference, as to the nature of the inquiry used. While a zero-inquiry certificate issued by "Certificates-R-Us" is, in some sense, a real certificate, its attestational value is low.

In practice, CAs will probably offer a range of certificates, graded according to the level of inquiry used to confirm the identity of the subject of the certificate. For example, VeriSign, a company that has recently begun advertising its willingness to provide identifying certificates[31] under the unfortunate name of

---

[29] Warwick Ford, Looking into the Crystal Ball: Certificates Revisited, Presentation at the Worldwide Electronic Commerce Conference (Oct. 20, 1995).

[30] *See* Ford, *supra* note 23, at 9. The Utah Act defines a "certificate" as a document that "names or identifies its subscriber." UTAH CODE ANN. § 46-3-103(3)(B). Arguably, this could be read to limit the reach of the Act to identifying certificates. Alternately, one could read the Act to say that any certificate that binds an attribute of the subscriber to the subscriber's public key "identifies" the subscriber in some manner. This seems the better reading since the Act clearly contemplates certificates other than identifying certificates, and even defines a "transactional certificate" as "a valid certificate incorporating by reference one or more digital signatures," UTAH CODE ANN. § 46-3-103(37), albeit stating a "transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference." UTAH CODE ANN. § 46-3-103(39)(B).

[31] Identifying certificates are described *infra* Part I.D.1.

"Internet driver licenses" for the information Superhighway,[32] proposes four different classes of certificates which will be compatible with Netscape World Wide Web browsers. Class 1 certificates, designed for "casual Web browsing and secure e-mail use," certify only "the uniqueness of a name or e-mail address."[33] VeriSign will issue Class 1 certificates in response to an e-mailed request by the subject.[34] In contrast, VeriSign will only issue a Class 2 certificate, which is more expensive, after receiving "third party proofing of name, address and other personal information provided in the on-line registration process."[35] To obtain a Class 3 certificate, the subject must pay still more money and appear in person or present "registered credentials."[36] VeriSign also contemplates a bespoke certificate, Class 4, that would issue after the subject is "thoroughly investigated."[37]

CAs are likely to issue several types of certificates, notably *identifying certificates*, *authorizing certificates*, *transactional certificates*, and *time stamps*.

1. Identifying Certificates

An identifying certificate, such as the ones being offered by VeriSign,[38] connects (the technical term is "binds") a name to a public key. The act of the CA in checking that the name corresponds to something in the nondigital world binds the name to an identity. Careful and accurate identification is not a trivial task: the cost of verifying the identities of all holders of U.S. Social Security cards and reissuing the cards would exceed $1.5 billion.[39] Of course, for digital communications, the "name" need not necessarily be either a unique name or even a real name.

---

[32] VeriSign, Class 1 Digital IDs, *available online* URL http:\\www.verisign.com\netscape\class1.html. The name is unfortunate because it implies that an identifying certificate is, or should be, a prerequisite to Internet access.

[33] *Id.*

[34] *Id.*

[35] VeriSign, Class 2 Digital IDs, *available online* URL http://www.verisign.com/netscape/class2.html.

[36] VeriSign, Class 3 Digital IDs, *available online* URL http://www.verisign.com/netscape/class3.html.

[37] VeriSign, Class 4 Digital IDs, *available online* URL http://www.verisign.com/netscape/class4.html.

[38] *See supra* text accompanying notes 32-37.

[39] Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 459 (1995) (citing *Hearing on the Use of the Social Security Number as a National Identifier Before the Subcomm. on Social Security of the House Comm. on Ways and Means*, 102d Cong., 1st Sess. 24-25 (1991) (statement of Gwendolyn S. King, Com-

The "name" could be "Darth Vader X" or "John Smith" or "John Smith, 1000 Main Street, Eugene, Oregon, Social Security Number 123-45-6789." In addition to being stored on computers connected to the Internet, certificates could be stored on smart cards, and could be used for issuing driver's licenses and public benefits, or conducting banking and other transactions.

In order to issue a certificate stating that a particular public key belongs to Alice, the CA generates an electronic message containing Alice's name, a statement as to the type of inquiry used to ascertain that the person purporting to be Alice is really Alice, and her public key. The CA signs this message with its private key. What happens next depends on the type of service the CA offers. The CA might publish the resulting certificate on a World Wide Web site available to anyone with Internet access, or give the certificate to Alice, or contract with Alice to honor e-mailed requests for the certificate from all comers. In some cases, these choices might affect the legal regime that applies to the CA.[40]

Armed with an identifying certificate from a reputable CA, Alice is in a much better position to persuade Bob that the digital signature she proffers really belongs to her and not to Mallet. If the CA is a reputable entity, and if its digital signature on the certificate can be verified,[41] Bob no longer has to trust Alice's electronic word because he now has confirmation from an independent source. Bob's attempt to verify the CA's digital signature requires that he have access to some independent means of ensuring that what purports to be the CA's public key is authentic, and not yet another scam by the cunning Mallet. Since the CA is in the business of providing such assurances, perhaps for a small fee, it may make economic sense for the CA to provide customers such as Alice and Bob with the means to confirm the authenticity of its public key, such as routine publication in a newspaper. The CA might also establish the accuracy of its public key by reference to a special "root" certificate established either by trade usage or by a government agency.

---

missioner of Social Security, estimating the cost of reissuing the cards from $1.5 to $2.5 billion)).

[40] *See infra* Part III.A.1.

[41] Recall that "to verify" a digital signature is to confirm that the public key associated with the party whose name appears on the message properly produces a numerical result that uses the plaintext as an input to the algorithm. *See supra* notes 19-20 and accompanying text.

Even a certificate that can be verified is not ironclad proof of an identity. For example, Bob might foolishly have shared the passphrase to his private key with a family member, who then takes advantage of this disclosure to make transactions under Bob's name. Bob's passphrase might have been carelessly chosen and cracked by Mallet. "Bob" might even *be* Mallet if the CA were negligent, or if Mallet is so good at fooling CAs that even the CA's reasonable care was insufficient to penetrate Mallet's deception.

The risks that the reality represented by the certificate is out of date can be controlled, but not eliminated, by ensuring that certificates are dated when issued, stated to have limited periods of validity or be subject to periodic reconfirmation by the CA, and by having Alice check the *certificate revocation list* (CRL)[42] maintained by the CA to warn recipients of certificates known to be no longer reliable. The absence of either rules or usages of trade determining who has a continuing duty to monitor the accuracy of data in certificate means that Alice has to make some difficult decisions. In addition to routinely checking the right CRL, Alice might decide that she will only accept certificates that state that their date of issue was within thirty days. If Alice is extremely cautious she can decide to accept only certificates that are very recent, maybe less than a day old, or even limit herself to certificates issued within minutes or microseconds. She still bears some risk, but it is reduced.

As for the risk of receiving an erroneous certificate, Alice will have to make a judgment as to which certificates from which CAs she will accept. This decision is likely to be based on the CA's reputation and on the representations that the CA makes about the level of inquiry undertaken to issue a certificate. To return to the VeriSign example,[43] Alice might decide not to accept "Class 1" certificates, but to require at least "Class 2." Or she might decide that there was something about the limitations on liability asserted by VeriSign that displeases her and so choose to refuse all its certificates because she prefers a competitor's promises. Whatever the level of inquiry promised by a CA, however, it is always possible that the CA was negligent or that Mallet simply outsmarted it. For Alice, these are the risks of the trade, much as

---

[42] *See* Ford, *supra* note 23, at 10. For more on CRLs see *infra* notes 107-08 and accompanying text.

[43] *See supra* notes 32-38 and accompanying text.

merchants bear some risk of forged signatures and counterfeit money in more mundane commerce.

2. *Authorizing Certificates*

Although identifying certificates are likely to be the most popular type of certificate in the short run, in the medium term CAs are likely to begin certifying attributes other than identity. An authorizing certificate might state where the subject resides, the subject's age, that the subject is a member in good standing of an organization, that the subject is a registered user of a product, or that the subject possesses a license such as bar membership. These authorizing certificates have many potential applications. For example, law professors exchanging exam questions on the Internet could require that correspondents demonstrate their membership in the Association of American Law Schools (AALS) before being allowed to have a copy of the questions.

It is illegal to export high-grade cryptography from the United States without advance permission from the federal government,[44] but there are no legal restrictions on the distribution of strong cryptography to resident aliens or United States citizens in the United States. The lack of a reliable means to identify the geographical location of a person from an Internet address creates a risk of prosecution for anyone making cryptographic software available over the Internet.[45] For example, if Alice is making high-grade cryptography available for distribution over the Internet, she might protect herself from considerable risk by requiring that Bob produce a valid[46] certificate from a reputable CA, stating that he is a United States citizen or green card holder residing in the United States, before allowing him to download the cryptographic software.

---

[44] *See generally* International Traffic in Arms Regulations, Pub. L. No. 90-629, 90 Stat. 744 (codified at 22 C.F.R. §§ 120-130 (1995)) (ITAR). The ITAR are administered by the Office of Defense Trade Controls in the State Department. If the State Department chooses, it can transfer jurisdiction of an export application to the Commerce Department. The statutory authority for the ITAR is the Arms Export Control Act (codified as amended at 22 U.S.C. § 2778 (1994)).

[45] Whether such a prosecution could succeed is a question beyond the scope of this Article. Since the instruction to download software is issued by the recipient's computer, an argument can be made that the "export" is committed by the recipient, not the owner of the software. In any case, the risks incident to being a test case are substantial: up to a $1 million fine and ten years in jail. 22 U.S.C. § 2778(c) (1994).

[46] For a discussion of what "valid" means in this context see *supra* text following note 42.

Alice substantially reduces her risk under the ITAR by requiring Bob to produce an authorizing certificate demonstrating his citizenship, but even this does not eliminate her risk. Alice's major remaining risks are that: (1) the CA's statement was erroneous; (2) Bob has lost control of his digital signature and it has fallen into the hands of Mallet, who is not a United States citizen or permanent resident, or is abroad; and (3) something about Bob has changed since he procured the certificate, for example, he has moved abroad, lost his citizenship or green card, or has died and his private key is held by his executor or heir.[47]

A certificate binding the geographic location, age, or other attribute to a public key can contain the name of the subject of the certificate, but the public key suffices if it was generated in a secure manner and is sufficiently long to be unique. Nameless, anonymous certificates create the possibility for sophisticated anonymous Internet commerce. For example, persons wishing to purchase materials that can only be sold to adults might obtain "over 18" certificates that bind this attribute to a public key but do not mention their name.[48] Similarly, a financial institution might issue a certificate linking a public key to a numbered deposit account.

3. *Transactional Certificates*

A third type of certificate, the transactional certificate,[49] attests to some fact about a transaction.[50] Unlike an identifying certificate or an authorizing certificate, a transactional certificate is not designed to be reused or to bind a fact to key. Instead, the certificate attests that some fact or formality was witnessed by the observer. For example, if Alice is a lawyer officiating at a digital closing, and Bob is her client, Bob can digitally sign a doc-

[47] Succession creates special problems for any system based on public-key cryptography. Any means Bob uses to create a backup copy of the pass-phrase to his private key introduces a new risk to his security. On the other hand, robust social protocols akin to those currently used in banking are needed to permit an executor or heir to enter into transactions that have been designed to require Bob's digital authorization.

[48] For an example of an anonymous age credentialing service targeting persons seeking access to "over 18" Web services, see Validate, *available online* URL http://www.zynet.com/~validate/services.html.

[49] Transactional certificates are sometimes referred to as *attesting certificates* or *notarial certificates*.

[50] The Draft ABA Digital Signature Guidelines define a "transactional certificate" as a "certificate for a specific transaction incorporating by reference one or more digital signatures." ABA Draft Guidelines, *supra* note 4, § 1.30.

ument. Alice then issues a certificate attesting that Bob digitally signed it in her presence. The certificate might contain the text of the document,[51] Bob's digital signature of the document, and Bob's public key, all of which would be signed with Alice's private key. The resulting certificate would be evidence that Bob affixed his signature in Alice's presence.[52] A transactional certificate of this type might suffice to transmit a deed to a public official for recordation.[53]

The differences between Alice's transactional certificate and Alice's digitally signed confirmation that she received Bob's document are primarily legal rather than technical. Indeed, from a cryptographic perspective, a transactional certificate is little more than an ordinary electronic document digitally signed with the CA's private key.

The potential legal differences are many and varied. First, the act of affixing the signature likely will carry with it the type of formality associated with a closing, or perhaps even with a notarial act in a civil law country. Indeed, the American Bar Association and the United States arm of the International Chamber of Commerce are exploring the creation of an American legal specialization to be known as a CyberNotary®.[54] A CyberNotary would be a lawyer able to demonstrate that she has the ability to issue certificates from a trusted computing environment. The hope is that civil law jurisdictions will come to accept a CyberNotary's certification as legally sufficient authentication and recordation of legal acts executed in the United States. If so, a power of attorney or the transfer of corporate shares certified by a CyberNotary in the United States would be recognized and enforced in those jurisdictions, even when an ordinary United States lawyer's or United States notary's certification would not

---

[51] Or, in some cases, a hash value, *see infra* text following note 59, and a pointer to the actual document.

[52] This example is drawn from the ABA Draft Guidelines, *supra* note 4, § 1.30.3.

[53] *See id.*

[54] In 1994, the Council of the ABA Section of Science and Technology resolved that its Information Security Committee should work with the ABA Standing Committee on Specializations to draft a proposal for ABA accreditation of the CyberNotary as recognized legal specialization. ABA Section of Science and Technology Section Minutes (Aug. 8, 1994) (copy on file with author). For updated information on the CyberNotary project see Theodore Sedgwick Barassi, *The CyberNotary: Public Key Registration and Certification and Authentication of International Legal Transactions*, *available online* URL http://www.intermarket.com/ecl/ cybrnote.html.

suffice.[55]

Second, a certificate will typically contain representations by the CA as to the level of inquiry conducted by the CA, or will at least incorporate a general policy statement by reference. In contrast, an ordinary digital signature adds no content to the message being signed.

Third, the CA may add link information to the document being signed, such as a secure timestamp from a trusted timestamping service.[56]

Fourth, by issuing a transactional certificate, a CA subjects herself to a completely different, and arguably far more benign, liability regime than does a CA who issues an identifying certificate. A transactional certificate is by nature a single-purpose certificate. While an unlimited and unknowable number of third parties may rely on it, the nature of their reasonable reliance is largely, perhaps completely, within the control of the CA. A lawyer who officiates at a closing, for example, might certify that she examined corporate documents and that the corporate officers were duly authorized to enter into the transaction; this is no different from what lawyers engaging in due diligence do today. It is, however, different from issuing an identity or creditworthiness credential to a person who might then use it to run up an unlimited amount of debt or other obligations.

4. Digital Time-Stamping Services

A *time stamp* is a cryptographically unforgeable digital attestation that a document was in existence at a particular time. It is not difficult to show that a document existed after another event: one need only include a reference to something that happened earlier, which could not have been predicted before it happened.[57] For example, before it became easy to doctor images, kidnappers could demonstrate that their victim was still alive by photographing him holding the front page of a newspaper. Sometimes, it is enough to prove that a document was signed or an event occurred after a given date, as in statute of limitations questions. Often, however, it is equally (if not more) important

---

[55] *See* Barassi, *supra* note 54.

[56] *See infra* Part I.D.4.

[57] Bayer et al., *supra* note 25, at 329. *See generally* Charles R. Merrill, The Digital Notary™ Record Authentication System—A Practical Guide for Legal Counsel on Mitigation of Risk from Electronic Records (June 22, 1995) (footnote omitted from title) (unpublished manuscript, on file with author).

to show exactly when it happened, or to prove that it happened before another date. If Alice quotes the headlines in last Tuesday's newspaper, it proves that she wrote the document no earlier than last Tuesday, but it gives Bob no way of telling whether she wrote it on any of the days since then. The "creation date" or "modification date" appended to documents by many word processing systems is also of little or no evidentiary value since it is a trivial matter to alter these dates, or to change the time on a computer's internal clock.[58] Alice's digital signature on the document tends to show that Alice wrote it and that no one else has altered it, but the signature adds nothing to the credibility of Alice's claim as to when she wrote it.

The only way to prove beyond doubt that a document was created before a certain time is to "cause an event based on the document, which can be observed by others."[59] If Alice publishes the text of her document in the newspaper, she can prove that it had to exist at the time it was published. This is expensive, uses a lot of newsprint, and destroys Alice's privacy. A better method is for Alice to publish a *hash value* of her document. A hash value is a large number produced by a *hash function* that takes the entire document as its input. The hash functions used in this manner have three properties that allow them to serve as a kind of fingerprint for a document. First, hash functions are public—anyone can repeat the calculation if he or she has the original document. Second, the hash function is a *one-way function*: if Alice sends Bob a file purporting to be the document that produced a hash value she published in the newspaper five years ago, Bob can easily confirm that the document's hash is the same, but possession of the hash value alone does not allow anyone to recreate the document. Third, although it is not impossible for two different documents to produce the same hash value, the odds against it are so high as to make this probability infinitesimal.[60] Therefore, even a slight alteration to a document will change its hash value, making it essentially impossible for Alice to create a document with the same hash value as the one whose hash value she published in the past. Even if Alice were to put supercomputers to work to find another set of bits that produced

---

[58] *See, e.g.*, Rudolph J. Peritz, *Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence*, 80 NW. U. L. REV. 956, 960 (1986).

[59] Bayer et al., *supra* note 25, at 329.

[60] *See* SCHNEIER, *supra* note 9, at 30-31.

the same hash value as the original digital document, there is no chance at all that this document would have letters and numbers in an order that produced intelligible text.

Of course, for most transactions it is impractical to rely on publication in a newspaper for authentication. This creates a business opportunity for CAs. Carol, a CA, can provide a simple time-stamping service by providing an attesting certificate that Alice sent Carol a hash value of a document at a certain time.[61] Carol might automate the process by having an Internet service that returned a dated and digitally-signed certificate every time a subscriber set her a hash value. Alice does not have to trust Carol with her data, because all Carol ever sees is the hash value. Now Bob no longer has to take Alice's word for when she wrote the document; he only need believe that Carol is telling the truth about Alice. If Carol is a reputable CA, her certificate may inspire this trust. If Bob is very mistrustful, however, he may be concerned that the system would fall apart if Alice can persuade Carol to backdate a time stamp.

A more secure method of time stamping documents exists. In this system, Bob does not have to trust Carol because there is no way for her to backdate a time stamp. Rather than simply signing the hash value of Alice's document, Carol sends Alice a digitally signed document reciting the hash values of Alice's document, the hash values of the last few documents submitted for time stamping and the e-mail addresses of their owners. Now, the only way to forge a time stamp is to suborn both Carol and many other users of the system. A weekly summary hash of the "tree" of the many documents submitted is published in the Sunday *New York Times* and is therefore unchangeable.[62] It is currently being marketed by its inventors as the "Digital Notary™."[63]

II

INTERNET COMMERCE: FRAUD'S PLAYGROUND?

Judging by the low amount of civil fraud (as opposed to crime) to date, the Internet's reputation as fraud's playground is undeserved. Yet, this may be the rare case in which expectations ac-

---

[61] *See id.* at 76.

[62] *See* Bayer et al., *supra* note 25, at 331-32.

[63] *See* Surety Technologies Homepage, *available online* URL http://www.surety.com; SCHNEIER, *supra* note 9, at 78-79; Merrill, *supra* note 57.

curately predict a possible future. While there may be a great deal of Internet advertising and information exchange, there are still relatively few transactions for value over the Internet. As the amount of Internet commerce grows, the opportunities for fraud may grow unless security and authentication measures also grow.

The CA's role in identification and authentication is particularly important for transactions that have effects which extend over time. In basic consumer transactions, where something is exchanged for money, there may be no need for certificates—a credit card suffices, with the issuer fulfilling the role of the third party. If the goods are not forthcoming or if they are other than they were represented to be, the customer can simply stop payment. If the goods are satisfactory, ordinarily the customer does not care whether the seller was who she claimed to be.

The picture changes dramatically, however, as soon as the transaction has lasting effects. If the communications are part of an ongoing relationship such as instructions to a broker, or if the terms of sale allow payments to be delayed, or if there is any question of a warranty or service contract, the parties have a much greater interest in identifying and authenticating each other.

A. Simple Sales

Although estimates vary, it is widely agreed that electronic commerce over distributed networks, such as the Internet, is set for explosive growth. One guesstimate suggests that approximately sixteen percent of consumer purchases may be electronic transactions by the turn of the century,[64] a date now about five years in the future. Definitions of electronic commerce differ; this Article concentrates on commercial activities such as sales and negotiations carried out over insecure distributed networks such as the Internet.

Internet commerce presents challenges that are not present, or are present in nearly harmless form, in traditional transactions carried out face-to-face. These problems include:

Basic Transactional Issues

- How to move value.

[64] Kelley Holland & Amy Cortese, *E-Cash Could Transform the World's Financial Life: Where E-Cash Will Take Off*, BUS. WK., June 12, 1995, at 66, 70.

- How to ensure that communications are secure from eavesdroppers.

Merchant's Desires

- AUTHENTICATION. Knowing the buyer's identity before making the sale may assist in proof of order and guarantee of payment. The merchant also may wish to build up a database of customers and their buying profiles.
- CERTIFICATION. The merchant may need proof that the buyer possesses an attribute required to authorize the sale. For example, some goods may only be sold to those licensed to use them; other goods require that the purchaser be over eighteen. Some products cannot be sold in some parts of the country, others cannot be exported.
- CONFIRMATION. The merchant needs to be able to prove to any third party involved in the transaction (such as a credit card company) that the customer did indeed authorize the payment.
- NONREPUDIATION. The merchant wants protection against the customer's unjustified denial that he placed the order, or that the goods were not delivered.
- PAYMENT. The merchant needs assurance that payment will be made. This can be achieved by having payment before sale, at time of sale, or by provision of a payment guarantee. A credit reference by a trusted third party provides a lesser form of assurance, but it at least demonstrates that the buyer is capable of making the payment.
- ANONYMITY. In some cases, the merchant may want to control the amount of transactional information disclosed to the customer.

Buyer's Desires

- AUTHENTICATION. Confirming the seller's identity prior to purchase helps ensure that goods will be genuine, and that service or warranties will be provided as advertised.
- INTEGRITY. Protection against unauthorized payments.
- RECOURSE. Comfort that there is recourse if the seller fails to perform or deliver.
- CONFIRMATION. A receipt.
- PRIVACY. Control over the amount of buyer/transactional information disclosed to third parties.
- ANONYMITY. Control over the amount of transactional infor-

mation disclosed to the merchant.[65]

Cryptographers would have us believe that most of the problems on this list that arise from Internet commerce and are not present in physical commerce can be solved, and the good news is that this is largely correct. The bad news, unless you happen to be a lawyer, is that the cryptographic solutions currently available are not simply mathematical. They frequently rely on the intervention of a trusted third party who is a certificate-issuing CA. Issuing certificates entails the creation of new entities, new businesses, and new relationships for which the duties and liabilities are currently uncertain.

The law of sales is complex, as the many sections of the Uniform Commercial Code (UCC) testify. Shifting any sale to an electronic medium can add further complexity. To better understand the nature of the new problems posed by electronic commerce, and the ways in which they are reduced by the introduction of a trusted third party, it helps to begin by considering this list of issues in the context of an extremely simple sale, one which includes no documents of title, and in which both goods and payment (or a promise to pay that functions as a close substitute, for example, a check or credit card transaction) are exchanged by face-to-face parties contemporaneously with the moment of contract formation.

1. Face-to-Face Sales

When Alice, a buyer, purchases food at the local grocery store from Bob, the merchant, in a face-to-face sale, there is no problem with moving value: Alice tenders paper money and coin,[66] food stamps or, if Bob permits it, Alice may choose to write a check, pay with an ATM card, a debit card, a credit card, or even in some cases buy "on account." Ordinarily, there is no particular need to ensure that the transaction is secure from Mallet, an eavesdropper, since there is little that Mallet could do with the information and even less that Mallet could do to hurt either Al-

---

[65] This list is an adaptation and simplification of the more formal and extensive list in Mihir Bellare et al., *iKP—A Family of Secure Electronic Payment Protocols* (July 12, 1995), *available online* URL http://www.zurich.ibm.ch/Technology/Security/publications/1995/ikp.ps.

[66] Payment in paper money or coin may create a demand for change. Problems may ensue if Bob lacks the correct change.

ice or Bob.[67] However, on the occasions when Alice and/or Bob would desire privacy or anonymity, they might find these difficult to obtain.

The documentation of the transaction differs slightly depending on whether it is a cash sale, or if there is a third party involved such as a bank or credit card company.[68] If there are just two parties, Alice and Bob typically keep copies of a receipt. If there is a third party, additional documents are generated, such as a check, an electronic ledger entry and a paper receipt in the case of an ATM card, or a credit card slip.[69] These pieces of paper also serve as proof of order in the unlikely event that it is questioned. Similarly, each of these payment mechanisms has well-developed ways of ensuring that consumers are protected from unauthorized payments.[70] On the other hand, buyer repudiation and nonpayment are issues in face-to-face commerce. A cash payment cannot easily be repudiated, but it may be counterfeit. A check can be dishonored by the bank, and under United States law, embodied in Regulation E, Alice has the right to contest a credit card payment up to two months later.[71]

Because physical goods are exchanged in a physical place, Alice has a number of indicators that suggest, although they do not prove, that she will have recourse in the event that the purchase is not satisfactory. First, Alice knows where the store is: its physical presence suggests that Bob may have assets that can be at-

---

[67] If Alice is careless, Mallet might be able to obtain Alice's credit card receipt, obtain her credit card number, and use it to run up charges on her credit card.

[68] The discussion in the text greatly simplifies reality to underline the differences between face-to-face commerce and electronic commerce. In the ordinary check sale, there may well be multiple banks, since at a minimum, the check is likely to be drawn on one bank, deposited to a second and cleared by a third. Similarly, some credit card transactions involve multiple parties.

[69] There is a significant difference between "on-line" clearance, in which Bob checks that the credit/debit card has sufficient credit/funds before authorizing the purchase, and "off-line" clearance, in which the purchase is not recorded with the credit card company until after the fact. In either case, transaction recording and customer profiling is possible if an electronic payment mechanism is used.

[70] For example, Alice's cash cannot be paid out unless it is stolen; checks cannot be drawn unless Alice's signature is forged, and even then the bank may have a duty to refuse payment. The holder of a credit card or debit card is only liable for the first fifty dollars fraudulently charged to the card. 15 U.S.C. § 1643(a)(1)(B) (1994); 12 C.F.R. § 205.6(b) (1995) (limiting consumer liability to $50 for most unauthorized electronic funds transfers).

[71] *See* 12 C.F.R. § 205.6(b)(2)(ii).

tached, even if only a lease and the contents of the shop.[72] The accessibility of the store's physical location also makes it easier for an irate customer to create bad publicity, either in the store itself or in the store's community, further creating an incentive for Bob to resolve any difficulty.[73] Furthermore, knowing the location of the store gives Alice an indication of the legal system that is likely to have jurisdiction over any conflict.

The physicality of the transaction also protects Bob. If authorization is required, Bob can demand that appropriate documents be displayed (for example, proof of age, unless Alice's appearance seems sufficient proof) and he can examine the credentials for authenticity. Bob also has some protection in the event that the transaction goes badly. Seeing Alice offers some chance of providing a description (or a store camera video) in the event of nonpayment or fraud. The face-to-face aspect of the relationship means that in many cases,[74] Alice will have to return the goods to claim reimbursement. Thus, typically Alice will be unable to continue to enjoy the products after claiming a refund.

2. *Telephone Sales*

Telephone sales lack the face-to-face aspect of a sale in a store. As a result, the parties are likely to have less knowledge about each other. In addition, telephone sales, like catalog sales, introduce a time lag between the order and its fulfillment, during which many things can go wrong: the goods may be discovered to be different from what the buyer had imagined they would be, the goods may spoil or be damaged in transit, either party may change its mind or become insolvent, and so on.[75]

The party who placed the call obviously knows the number she dialed, although if Alice calls Bob via an 800 number, that telephone number alone reveals little or nothing about Bob's location.[76] The recipient of the call may also know the calling party's number if caller ID is available. Indeed, calls to an 800 number

[72] The shop suggests, but does not prove, that Bob has attachable assets, since these assets may be encumbered by liens and mortgages with priority.

[73] Other than bad publicity, most jurisdictions limit Alice's self-help remedies in the event of a dispute.

[74] Consumables, perishables, and easily-copied materials excepted.

[75] The UCC supplies a large variety of techniques that address each of these problems, and more. *See generally* RICHARD E. SPEIDEL ET AL., SALES AND SECURED TRANSACTIONS 452-60 (1993).

[76] Indeed, some firms, notably airlines, commonly switch calls from 800 numbers to operators located abroad. Catherine Cleary, *Telemarketing Harnesses Technology*

automatically disclose the number of the calling party.[77] If Bob uses a database indexing telephone numbers to addresses, credit histories, or buying patterns, he may have considerable information about Alice regardless of who places the call. On the other hand, if Alice is an ordinary consumer, her information about Bob will depend largely on sources extrinsic to the call (for example, catalogs, advertising, prior dealings) and the firm's reputation, if any. In addition, returning goods or getting redress may be more difficult with a faraway party. Not only may the relevant legal system be inaccessible or expensive to access, but Alice's inability to bring her complaint to the attention of other shoppers reduces her bargaining power with Bob.

Although impersonation is certainly possible at the grocery store,[78] it is easier over the telephone. Lacking the ability to verify signatures or identify the physical characteristics of the buyer, Bob runs an increased risk of making sales to persons using stolen credit card numbers (although this risk is attenuated by using on-line clearing). Similarly, because it is difficult to verify identity over the telephone, Alice runs an increased risk that the person claiming to be Bob is actually Mallet.

Although value cannot be exchanged by cash or check at the time of sale, mailed payment can be a prerequisite to shipment. As a practical matter, consumer telephone sales tend to be made by debit or credit card because this medium of payment gives the merchant considerable assurance of Alice's ability to pay, but not necessarily a guarantee that payment will actually be made. The credit card company's inability to ensure nonrepudiation[79] becomes a positive advantage, because Alice can transact knowing that payment can be suspended if Bob, or the person claiming to be Bob, fails to perform in some material way. Similarly, the ability to repudiate transactions means that while the call may be subject to eavesdropping or diversion, these acts are of limited value to a third party so long as Alice checks her credit card bill

---

and Blarney, IRISH TIMES, Dec. 29, 1995, at sec. 3, supp. 7 (LEXIS, News Library, Curnws file).

[77] *See* Edmund L. Andrews, *New Rules Are Approved for Nationwide Caller ID*, N.Y. TIMES, May 5, 1995, at D5.

[78] As the volume of trademark infringement suits demonstrates, goods as well as people can be inauthentic.

[79] *See supra* note 71.

carefully for unauthorized purchases.[80]

3. *Internet Sales*

Internet sales are likely to take two general forms: ordinary commerce in tangible things and information commerce.

Ordinary commerce in tangible things will greatly resemble common transactions today: purchases that are currently carried out by telephone, ordinary mail (for example, catalog sales) and even in person. Ordinary rules of commercial law presumably will continue to apply to these transactions, subject to one vital difference: without taking some special measures to identify each other, the parties will be saddled with a risk that their counterpart will not be who she professes to be. Transactions that use a telephone require that someone dial a telephone number. The use of that telephone number implicates a record that ultimately could identify the party called. In some cases, the number alone will provide the identification; in other cases, it may be necessary to invoke the aid of the legal process, or of the telephone company. Nevertheless, the telephone number provides some kind of link to a physical presence, for at least one of the two parties to the communication.[81] An Internet e-mail address, by contrast, gives the recipient no reliable information about the person sending the message.

Information commerce is more of a departure from traditional sales. It has the immediacy of a face-to-face transaction, but little mutual identifying information need necessarily be exchanged. In information commerce, unlike ordinary commerce in tangible things, there may be no package to help identify the sender after the goods are delivered. Instead, both parties will conduct the exchange electronically: the buyer will send digital cash and the seller will send information.[82] Some of these transactions may be sizable, such as the sale of access to proprietary databases or the purchase of computer software, but others are likely to be very small. For example, providers of information on the World Wide Web might choose to charge a fraction of a penny to each person

---

[80] Typically, merchants do not receive payment from a credit card sale until the repudiation period has passed.

[81] The call record may also identify the caller, but this is less certain. The caller could place the call from a pay phone.

[82] Whether the exchange is performed simultaneously or in series is up to the parties.

accessing their pages.[83] Browsers may be configured to pay these charges, up to a predefined limit, without ever troubling the user. Existing credit card systems are too expensive for such microcharges.[84] Microcommerce in information will require a digital payment system that does not rely on the (expensive) participation of a third party such as a credit bureau or credit card issuer.[85] If such a payment system could be widely deployed, the potential for growth of Internet information commerce is enormous.

Identifying or authenticating certificates can provide all the information that a party might reasonably want for both information commerce and ordinary commerce in tangible things. Whether it makes sense to require a certificate at all depends on the amount of the transaction, the mode of payment, and the cost and delay associated with use of a certificate. Of course, even when it makes sense to use a certificate to verify identifying information about a transactional counterpart, this serves only to restore the parties to an informational position akin to what is commonplace in other more familiar transactions. It does not in any way reduce the need for the existing, and complex, rules about consideration, delivery, breach, title, security interests, fraud, or any of the myriad other things addressed by the UCC and other commercial and criminal law.

a. Transactional Issues: Moving Value and Authentication

If Alice has no hardware available to her other than her computer,[86] she can choose to move value to Bob across the Internet

---

[83] *See* Arnold Kling, *Banking on the Internet*, *available online* URL http://www-e1c.gnn.com/gnn/meta/finance/feat/archives.focus/ bank.body.html.

[84] *See*, *e.g.*, Electronic Cash, Tokens and Payments in the National Information Infrastructure § 1.1, *available online* URL http://www.cnri.reston.va.us:3000/XIWT/documents/ dig_cash_doc/ElecCash.html. The average U.S. credit card purchase today is $60. *Id.*

[85] Steve Glassman et al., *The Millicent Protocol for Inexpensive Electronic Commerce*, *available online* URL http:// www.research.digital.com/SRC/millicent/papers/millicent-w3c4/millicent.html, argues that even digital coins are too expensive for microtransactions, and that a new form of "scrip" needs to be deployed for microtransactions. Proposals for two schemes that may meet the exacting requirements of efficient micro-transactions can be found in Ronald L. Rivest & Adi Shamir, *Payword and MicroMint: Two Simple Micropayment Schemes* (Apr. 3, 1996), *available online* URL http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps.

[86] Smart cards, sometimes called electronic wallets, also can be configured to be stores of value. Rather than digital cash embodied in "coins" that are a series of numbers in a cryptographic envelope, an electronic wallet contains a counter that

with a debit card, a credit card, or electronic cash.[87]

(i) Debit Cards and Credit Cards

Today, the simplest way for Alice to pay Bob across the Internet is to use a debit card or credit card. This payment mechanism has the great virtue of familiarity. It uses established mechanisms to apportion risk of nonpayment and repudiation. Although it is vulnerable to eavesdropping, the risk may be smaller than commonly believed.

If Alice sends out unencrypted credit card information on the Internet she takes a chance that a third party will intercept the information. To date, however, there are no reported cases of credit card information acquired by eavesdropping on an Internet transaction being used to make a purchase.[88] When one considers that the same credit card information is easily available to every employee of every merchant who accepts credit and debit cards, and can be acquired by examining paper credit card slips retained by any restaurant or dumped in the trash at any mall, it is easy to see why few people go to the considerably greater trouble of attempting to obtain credit card numbers by monitoring large volumes of Internet traffic.

If Alice wants greater security, she can encrypt her credit card data before sending it. Similarly, Bob may want assurances that Alice is who she purports to be. Bob may want Alice to send her order encrypted with her private key, thus uniquely identifying the order as emanating from her. For a greater level of security, Alice and Bob may require that identifying certificates from a

---

records the amount of money held on the card. Movement of value on and off that counter can be hedged with a number of cryptographic safeguards. For example, cards can be programmed to only accept value from cards that properly identify themselves. Smart cards can be used to transfer value across the Internet if both parties to the transaction have smart cards or the equivalent, and both have computers outfitted with appropriate card readers. For a taxonomy of smart card types see David Chaum, *Prepaid Smart Card Techniques: A Brief Introduction and Comparison*, *available online* URL http://ganges.cs.tcd.ie:80/mepeirce/Project/Chaum/cardcom.html.

87 One can also imagine other, less practical, systems, including barter transactions, by which Alice and Bob exchange services or digitizable products (software, poems).

88 In contrast, in one incident, credit card information belonging to more than 20,000 customers that had been stored in an insecure database was compromised. *See* JONATHAN LITTMAN, THE FUGITIVE GAME 325, 348 (1996) (reporting apparent copying of credit card records by Kevin Mitnick).

reputable CA accompany the exchange of public keys.[89] On the other hand, since the debit/credit card issuer/administrator fulfills some of the functions of a trusted third party already, and charges the same commission regardless of whether Alice and Bob exchange certificates, they may decide to take the risk.[90]

Although debit and credit cards are the easiest means of transferring value over the Internet, and require little if any legal innovation, they have some disadvantages as well. Neither debit nor credit cards are suited to small transactions because verification and clearing impose significant fixed costs on every transaction.[91] Because one of the most likely applications of Internet sales is microcharges—pennies or fractions of a penny—for the right to view information such as a World Wide Web page, this inability to handle tiny transactions strongly suggests the need for an alternate payments mechanism. Furthermore, the utility of credit and debit cards is critically dependent on the continuing applicability of the consumer's liability being capped at fifty dollars in the event that a credit card number is copied in transit or misused by the recipient. Without the fifty dollar limit, Alice would face an enormous danger of her credit card information going awry, either because Mallet managed to penetrate Bob's security and copy all messages as they were sent to Bob's store, or because Mallet fooled Alice into sending him the credit card information by pretending to be Bob, or because Bob was careless and Mallet hacked his database. Any change in this regulatory regime would cause Alice, and indeed all consumers contemplating electronic transactions, to need both encryption and authentication.[92]

---

[89] Alternately, Alice and Bob may find each other's public keys on a keyserver that is part of the National Information Infrastructure; the keyserver may itself demand a valid certificate as a condition of the listing, or it may contain (optional?) pointers to the databases where the certificates reside.

[90] The risk is not negligible; the consumer risks a fifty dollar charge, 12 C.F.R. § 205.6(b), and considerable hassle, plus potential damage to a credit rating. The merchant takes the risk of nonpayment since the credit card company will not pay the merchant if the customer fails to pay.

[91] *See, e.g.*, Stefan Brands, Centrum voor Wiskunde en Informatica (CWI), *Offline Electronic Cash Based on Secret-Key Certificates* 1-2 (Report CS-R9506 1995), *available online* URL ftp://ftp.cwi.nl/pub/brands/CS-R9506.ps.Z.

[92] Whether Regulation E should apply to electronic money has been a matter of some debate in Congress. *See, e.g.*, *Bill's EFTA and Reg E Exemptions Need Reworking, Blinder Tells Panel*, BNA BANKING DAILY, Oct. 12, 1995, at *2 (LEXIS, News library, Curnws file). ("Blinder said that he could support an extensive, and perhaps blanket exemption from Reg E for stored-value cards of $20, but that there

(ii) Electronic Cash

Electronic cash implementations vary.[93] While generalizations are hazardous, most true digital cash systems that are entirely software-based (for example, do not rely on a smart card or other physical token to provide authentication or to store value) use some variation of the "digital coin." A digital coin is a sequence of bits, perhaps signed with an issuing financial institution's private key, that represents a claim of value.[94]

Software-based digital coins are potentially suitable for small transactions, such as charging a penny or less to view a web page, where credit cards would be prohibitively expensive.[95] Unfortunately, since bits are easy to copy, digital coin schemes require fairly elaborate mechanisms to prevent a coin from being spent more than once. One method of preventing double spending is to require that coins be cleared in real time. If Alice offers a coin to Bob, Bob immediately accesses the issuing bank to make sure that the coin is valid and has not previously been spent.[96] A necessary consequence of this protocol is that if Alice uses a digital coin to pay Bob, Bob cannot spend it directly. Instead, Bob must either deposit the coin in an account at the issuer or turn it in for another digital coin or conventional money.[97] An on-line clearing system can be configured to ensure that the bank does not know who gave Bob the coin (payor anonymity), but the bank will know that Bob received the coin (no payee anonymity).

While Bob might clear large payments from a single source on line by making a real-time connection to the bank to ensure that

---

are questions about whether such an exemption is appropriate for large amounts transferred over computer networks.").

[93] *See, e.g.*, PETER WAYNER, DIGITAL CASH: COMMERCE ON THE NET (1996) (surveying a large number of existing and proposed systems); Froomkin, *supra* note 21, at Part III.B.2 (surveying fewer systems in more detail).

[94] *See generally* Froomkin, *supra* note 21, at Part III.B.

[95] Charging and payment might be built into the browser. Alice might program her browser to pay any fee up to a set amount, say two cents, without asking for confirmation. Glassman argues that even digital coins are too expensive for micro-transactions, and that a new form of "scrip" needs to be deployed for micro-transactions. *See* Glassman et al., *supra* note 85.

[96] One United States financial institution currently offers a "DigiCash" implementation with real money. *See* Mark Twain Banks, Providing Global Investment Solution, *available online* URL http://www.marktwain.com.

[97] *See* David Chaum, *Achieving Electronic Privacy*, SCI. AM., Aug. 1992, at *1-2, *available online* URL http://ganges.cs.tcd.ie/mepeirce/Project/Chaum/sciem.html (discussing electronic cash); Ecash Homepage, *available online* URL http://www.digicash.com/ecash/ecash-home.html.

the coins have not previously been spent, this may be impractical and uneconomic for transactions measured in pennies or less. Instead, Bob will accumulate a hoard of small digital coins and send them to the bank to clear in batch lots. This off-line clearing opens a window of opportunity for unscrupulous parties to engage in multiple spending. In order to forestall this, a bank issuing coins that will be redeemed off-line is likely to require that Alice encode some identifying information about herself onto the coin. The system can be set up so that no one, not even the bank, can read this information so long as Alice spends the coin only once. A second attempt to spend the coin will disclose Alice's identity and allow the issuer to sue her for fraud and perhaps report her to the authorities for criminal charges of fraud or theft.[98] Barring a complex money-laundering protocol,[99] Bob cannot respend this type of coin either, and must turn it into the bank just as if it had been cleared on-line.[100]

This feature reduces the need for Alice and Bob to exchange certificates; in essence, the digital coin carries its own certification. If Bob is particularly concerned about the possibility of double spending, or if the percentage of respent coins being tendered to Bob reaches unacceptable levels, Bob may choose to restrict even his microsales to parties that can provide an identifying certificate. Bob's decision will turn in part on the cost and delay associated with a certificate as opposed to the cost and delay of having the bank help him trace double spenders.

b. Confirmation Issues: Proof of Order, Nonrepudiation, Receipt, and Recourse

All that Alice needs in order to prove that Bob made a promise to buy or to pay is a message including the promise signed with Bob's digital signature.[101] The issue of proving the promise is separate from whether a digital signature is a "signature" for

---

[98] If the coins are cleared off-line, and the double-spender has received value from the payee, then there is clearly theft from the payee. Whether the double spender can be charged with attempted theft from the bank may depend on whether the relevant jurisdiction allows prosection for attempted "impossible" crimes. Since in most protocols the bank checks the validity of every coin before exchanging it for value, there was no possibility that it would actually suffer a loss; the offense against the bank is thus "impossible," and in some jurisdictions arguably noncriminal.

[99] *See infra* text accompanying notes 102-04.

[100] *See* Froomkin, *supra* note 21, at part III.B.3.

[101] Electronic writings ordinarily satisfy the Statute of Frauds. *See* John R. Thomas, Note, *Legal Responses to Commercial Transactions Employing Novel Com-*

legal rules that require that a writing bear a signature.[102] Alice will find it less cumbersome to prove Bob's promise if she has access to a certificate, valid at the time of Bob's promise, that links Bob to the signature appearing on the message. However, a certificate may not be strictly necessary depending on the payment mechanism and the nature of the transaction.

Debit and credit cards leave an information trail that can assist Alice in finding Bob, and vice versa. Because a payor might have an anonymous or pseudonymous debit/credit card,[103] or because a payee might have disappeared in the time since the transaction was recorded, the trail is not perfect. However, the trail of information is significant, and not much different from what would likely be in a certificate, so it is likely to make the certificate somewhat redundant.

Digital cash can be designed to protect the anonymity of the payor who does not double spend. A prudent payee who is tendered digital cash with this anonymizing feature may seek an identifying certificate from the payor if the transaction makes it important to know her. As most digital cash schemes do not protect the anonymity of the payee, the payor will request an identifying certificate only if the cost of the certificate is less than the expected value of the cost of persuading the bank to release the payee's identity on an occasion where this might be needed, adjusted for the danger that the payee will get away before being identified. The cheaper and quicker it is to use a certificate, the more likely it will be used.

The introduction of a coin laundry service that offered payees an opportunity to exchange coins anonymously would greatly increase the payor's need for a certificate from the payee. A coin laundry would break the guaranteed link between the identity of the payee and the coin, whether or not Bob actually avails himself of the service. If Alice knows that Carol's coin exchange is in business, Alice will have to be more wary about sending coins to Bob, a stranger. Now, if Bob takes the coin and defaults on the

---

munications Media, 90 MICH. L. REV. 1145 (1992); Merrill, *supra* note 57, at 3. A digital time stamp may add evidentiary value. *Id.* at 1.

[102] Whether a digital signature is a "signature" is beyond the scope of this article. *See generally* BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE § 16 (2d ed. 1995).

[103] For a description of how to obtain an anonymous credit card, *see, e.g.*, Vaxbuster, *Safe and Easy Charging*, 4 PHRACK Issue 44, File 20, *available online* URL http://www.fc.net:80/phrack/files/p44/p44-20.html.

transaction, it is no longer obvious that the bank will be able to identify Bob when Alice asks it to reveal who redeemed her coin. If the bank tells her that the coin was redeemed by Carol's money changing service, and Carol's service is located in a foreign jurisdiction, perhaps one with strong bank secrecy laws,[104] Alice may find it very difficult to find out who Bob really is and where he lives. In these circumstances, Alice may find that she wants an identifying certificate from Bob after all.[105]

Consumers will have an increasing need for anonymous commerce as merchants become more adept at assembling computerized databases on their customers, and as these databases themselves become valuable commodities.[106] Anonymous certificates are likely to play an essential role in anonymous commerce since they will help induce parties to trade with one another when they are unable to identify each other.

B. Ongoing Transactions

As we have seen, there is a somewhat reduced need for a CA's services when payment and goods are exchanged simultaneously, although the need for a trusted third party is not eliminated. In part this is because the payment schemes already incorporate a trusted third party—the credit card company or the digital cash issuer—who is likely to be capable, if pushed, of providing some identification of the defaulting party in the event the transaction goes badly.

In contrast, any communication in which the exchange of funds and goods is not immediate, or which looks either backwards or forwards in time, creates a strong and continuing need for authentication and/or identification. For example, if Alice has an account with a broker, Bob, both Bob and Alice have a strong interest in ensuring that any buy or sell order regarding Alice's account be from Alice and no one else, and that this fact be easily provable should it ever be called into question. Similarly, par-

---

[104] Banks are increasingly unwilling to provide truly anonymous bank accounts. *See, e.g.*, William W. Park, *Anonymous Bank Accounts: Narco-Dollars, Fiscal Fraud, and Lawyers*, 15 FORDHAM INT'L L.J. 652, 668-69 (1991-92). Governments are increasingly unwilling to allow banks based within their regulatory reach to offer this service, in part because of the Council of Europe Money Laundering Convention whose reach extends beyond Europe. *See* EuroWatch, *Banking Secrecy: Liechtenstein Signs European Money Laundering Convention* (July 28, 1995) (LEXIS News library, Curnws file).

[105] I am greatly indebted to Hal Finney for alerting me to this scenario.

[106] *See* Froomkin, *supra* note 21, at part IV.

ties negotiating on the Internet will want to ensure that they know who they are communicating with in order to keep secrets from their rivals. No supplier will wish to accept orders for goods that are sold on terms that allow payment at a future date, even from a regular customer, without assurances that the key used to sign the order is one belonging to a person authorized to place the order.

It is important to recall that, much like in the nonelectronic world, the authentication/identification problem in these circumstances has two parts. Bob wants a certificate showing that Alice is who she says she is and/or that Alice is authorized to do what she wants to do. In addition, Bob needs an assurance that the certificate issued to Alice remains valid. Alice could have left her job as purchasing agent or she could have discovered that someone has learned her passwords. In the nonelectronic world, customers frequently take these things on faith; in the electronic world, such faith is less reasonable and thus likely to be less frequent.

In order, therefore, to be willing to rely on a certificate issued to Alice for transactions of any value, Bob needs easy access to a CRL[107] that will allow him to establish that Alice's certificate has not been revoked or suspended. When Alice shows Bob her certificate (or when Bob contacts Carol to get a copy of Alice's certificate) Bob—or Bob's software—will check to see whether the certificate has been revoked,[108] much like credit cards are checked against lists of suspended cards today. Bob thus needs an easy way to identify and get access to the CRL that would list Alice's certificate if there were something wrong with it. And every CA needs an efficient and reliable means of communicating its CRL to potential users of certificates.

Fortunately, the means for achieving these ends are now at hand. The recognized standard for certificates is the X.509 standard maintained by the International Telecommunications Union

---

[107] *See supra* text accompanying note 42 (describing the Certificate Revocation List).

[108] A certificate also might be suspended for a brief period, pending inquiries as to whether it should be revoked. A prudent CA that received an emergency telephone call asking that a certificate be revoked might suspend it while waiting for proof that the person making the request had the authority to do so. *Cf.* UTAH CODE ANN. §§ 46-3-306, -307 (providing for suspension of a certificate).

(ITU).[109] Previous editions of this standard defined a relatively rigid and inflexible form for a certificate, one that was not well-suited to the legal requirements of digital commerce. In particular, neither the original X.509 standard, nor the revision known as X.509 (ver 2) made provisions for a certificate to carry information about the CRL. Instead, the original X.509 standard provided information about how to contact the CA, and the user was expected to be able to use this information either to identify the CRL or to contact the CA for more information.[110] A recent change in the X.509 standard, now known as X.509 (ver 3), solves these problems. The new standard defines a data location where a CA can put information that will allow Bob to find the CRL quickly, such as the Internet address (URL) of the applicable CRL.[111] The new standard, which is being mirrored in standards developed by ANSI X9 (which adopts standards for banks) and ISO/IEC, also includes a data field in which a CA can insert information about how to find the policies that apply to the certificate, such as the level of inquiry undertaken before issuance.[112]

III

The Difficulty of Identifying the Rights and Duties of Private Certification Authorities

As electronic commerce grows, it will become increasingly important to define the rights and duties of CAs. This will not be an easy task, particularly once electronic commerce becomes more international. International transactions intensify the problems caused by the divergences between legal systems and tend to raise the stakes in choice of law.[113] "The consumer cannot and indeed *will* not participate effectively in the . . . market where economic and legal conditions are obscure."[114] Although

---

[109] Ford, *supra* note 23, at 9. The ITU was formerly known as the Consultative Committee on International Telephony and Telegraphy (CCITT).

[110] *Id.* at 10, 11.

[111] *Id.* at 12-14.

[112] *Id.* at 13.

[113] Peter Sutherland, *The Internal Market After 1992: Meeting the Challenge, Report to the EEC Commission by the High Level Group on the Operation of Internal Market* (1992), identified consumer uncertainty as a major impediment to the realization of a single European market.

[114] Stephen Weatherill, *The Role of the Informed Consumer in European Community Law and Policy*, 2 Consumer L.J. 49, 59 (1994).

international issues are beyond the scope of this Article,[115] identifying and applying the relevant substantive law can be a moderately complex problem even when the focus is restricted to one state in the United States.[116]

The duties and potential liabilities imposed on private[117] CAs by United States law are unclear, as might be expected from the dearth of applicable legislation,[118] the complete absence of case law, and the very small number of currently functioning CAs. Legislation attempts to provide clarity: the Utah Digital Signature Act provides for a safe harbor against most liability for those CAs who qualify. No CAs have qualified to date, and the Act in any event does not define the duties and liabilities of CAs who do not qualify for the safe harbor.[119] Clarification of the duties and liabilities of these CAs in the absence of legislation should thus serve the interests of all parties to an electronic transaction in which a certificate plays a role. As other legislatures debate whether to enact digital signature laws of their own, they may find it helpful to have a better understanding of the legal background against which they are working. This Part seeks to begin a discussion of that background by addressing a sample problem: who, under existing law, is liable for an erroneous certificate.

The importance of clarifying a CA's liabilities will grow further if one aspect of the recently passed Utah Digital Signature Act becomes a national model. If Alice wants to persuade a jury that the pen-and-ink ("holographic") signature on a contract or note is in fact Bob's, but Bob claims that it is a forgery, Alice must bear the burden of proving that Bob's signature is genuine. Digital signatures are nearly impossible to forge, and the Utah Digital Signature Act thus reverses the presumption of authenticity for digital signatures. Under the Utah Act, a digital signature that can be verified by a valid certificate is presumed to belong to

---

[115] For a discussion of the likely reception of digital signatures in Canadian law, see Serge Parisien, *Aspects Juridiques et Technologiques des Mécanismes de Signature Électronique: Une Analyse Comparative*, *available online* URL http://www.droit.umontreal.ca/Palais/Invites/AQDIJ/Colloque_10_11_95/ Parisien/parisien_udm.html.

[116] Because this Article already exceeds the length limits suggested by the editors of this symposium volume, it does not include any discussion of choice of law issues.

[117] For a discussion of the liabilities of a public CA, see BAUM, *supra* note 22.

[118] *See supra* note 4.

[119] *See supra* notes 6-8. As this Article went to press, Utah was joined by the State of Washington. *See supra* note 4.

the subscriber listed in the certificate.[120]

Utah's presumption means that Alice can have greatly increased confidence in the enforceability of Bob's digital signature so long as Alice can verify Bob's digital signature with a valid certificate issued by a registered CA. This increased confidence could be of great value in everything from automated microtransactions to large international transactions where the parties are strangers.

On the other hand, the presumption creates a danger for a consumer who loses control of his digital signature. Although implementational details will vary, most digital signatures are likely to be protected with at least a passphrase, a more complex version of the PIN number that protects most bank cards today. Some digital signatures may require both a passphrase and a hardware token (for example, a smart card), or even the passphrase, the hardware token, and a biometric authentication (for example, a thumbprint scan). In the absence of the most heroic biometric security measures, however, the consumer is at risk that someone will acquire the hardware token and either guess the passphrase or obtain it by eavesdropping or some other means. If this happens, the Utah legislation creates a spectre of unlimited liability that can only be capped once the consumer reports that the digital signature has been compromised. Since there is likely to be a lag between loss of control of the signature and discovery of that fact, a reasonable consumer might well choose to avoid this risk by not creating a digital signature at all.[121] Utah's presumption seems considerably less unreasonable when applied to large sophisticated organizations using the signatures for substantial transactions.

A. Liability for Erroneous Certificates

Inevitably, certificates will issue with false statements, and third parties will rely on them to their detriment. In the absence of much state[122] or federal regulation, it will fall to the courts to determine who should bear the liability when this happens. They will have a difficult task.

---

120 UTAH CODE ANN. § 46-3-406 (1996).

121 *See* Benjamin Wright, Eggs in Baskets: Distributing the Risks of Electronic Signatures, *available online* URL http://www.sig.net/~jbc/signatur.html.

122 *See supra* note 4 for a summary of state legislation to date.

1. Is a CA Selling a Good or a Service?

The difficulties in determining a CA's duties and liabilities begin with how one characterizes the CA's provision of a certificate: is the CA providing an investigative "service" of which the certificate is an embodiment or memorial—much like a lawyer's opinion letter or a valuer's opinion—or is the certificate that the CA is selling a "good," or is the transaction a mixture of a good and a service? The characterization determines whether Article 2 of the Uniform Commercial Code (UCC) applies to the CA's provision of a certificate.

If the CA is selling a "good," then Article 2 of the UCC applies.[123] If Article 2 applies, it brings with it a menu of default rules, as well as provisions for statutes of limitation and express and implied warranties including, in particular, the implied warranty of merchantability[124] and the warranty of fitness for a particular purpose.[125] Article 2 of the UCC also imposes limits on the disclaimers of those warranties.[126] Article 2 of the UCC is not, however, uniform in ways that would matter greatly to CAs, their customers, and relying third parties. For example, section 2-318 of the UCC offers states a choice of three different rules governing the seller's warranty liability to third parties. One version of section 2-318 limits the run of the CA's warranties to persons in the family or household of the buyer,[127] but leaves the common law unchanged as to the effect of the warranty on "other persons in the distributive chain."[128] A CA in such a state will have whatever liability to third parties the common law of the state imposes: for example, the liability for negligent misrepresentation discussed below. The UCC's second version of section 2-318 extends the run of the CA's warranties to all natural persons "who may reasonably be expected to use . . . or be affected by the goods."[129] CAs subject to this provision will find that they are subject to warranty claims for "defective" (that is,

---

123 U.C.C. § 2-102 (1994); *see also* note 132.

124 U.C.C. § 2-314.

125 U.C.C. § 2-315. An example of a claim under section 2-315 might be against a CA that had provided a certificate signed with an insecure key or a key known to be compromised.

126 *See* JAMES J. WHITE & ROBERT S. SUMMERS, UNIFORM COMMERCIAL CODE ch. 12 (4th ed. 1995).

127 U.C.C. § 2-318, alternative A. This alternative is the most commonly used of the three. WHITE & SUMMERS, *supra* note 126, at 392 n.3.

128 U.C.C. § 2-318, cmt. 3.

129 U.C.C. § 2-318, alternative B. This alternative is the least frequently used of

erroneous) certificates to all natural third parties, since the reliance of such third parties could reasonably be expected. The UCC's third version of section 2-318 includes artificial as well as natural persons among the third parties who can make warranty claims.[130] CAs in such states will provide the certificates that should, all other things being equal, command the most trust; they also will face the largest potential liability. The problem from the point of view of a person trying to decide whether a certificate is reliable is that they will not necessarily know which of these provisions happen to apply unless the certificate tells them. In addition to the three official versions of section 2-318, a number of states use formulations of their own, further complicating matters.[131] If the UCC applies to the sale of a certificate, this lack of uniformity could impose a large burden on Bob when Alice asks him to accept Carol's certificate. Unless Bob and Alice happen to live in the same state as Carol, they will need to know which state's law applies, and whether that state's law allows Bob to take comfort from Carol's express and implied warranties about the reliability of her certificate.

If, on the other hand, the CA is selling a "service," then the UCC Article 2 is by its own terms inapplicable.[132] It is not obvious that Article 2 should apply to the provision of a certificate. UCC section 2-105(1) defines "goods" as "all things . . . which are moveable at the time of identification to the contract for sale other than the money in which the price is to be paid, investment securities . . . and things in action."[133] Since a certificate is highly movable, it might seem to be a "good" under this definition. This temptation should be resisted: a certificate is only a little closer to the classic definition of a "movable good" than is a surveyor's or valuer's report. A certificate resembles a professional's opinion in that a certificate ordinarily is the tangible memorial of a

---

the three, but it has been adopted in six states. WHITE & SUMMERS, *supra* note 126, at 393 n.6.

[130] U.C.C. § 2-318, alternative C. This alternative, or some form of it, is used in at least eight states. WHITE & SUMMERS, *supra* note 126, at 393 n.7.

[131] WHITE & SUMMERS, *supra* note 126, at 393 n.8.

[132] *See* U.C.C. § 2-102 ("Unless the context otherwise requires, this Article applies to transactions in goods . . . ."). Proposed revisions to Article 2 may extend its coverage to include "service contracts." *See* Raymond T. Nimmer, *Intangible Contracts: Thoughts of Hubs, Spokes, and Reinvigorating Article 2*, 35 WM. & MARY L. REV. 1337, 1374, 1389 (1994). This change would greatly increase the likelihood that Article 2 applies to the provision of a certificate.

[133] U.C.C. § 2-105(1).

process of analysis in which the subject's credentials were checked in some manner. On the other hand, a certificate differs from a professional's opinion in some ways that may be relevant. Any trustworthy CA will be managed by a professional—someone who knows how to run a trustworthy computer system—but it is not inevitable that the actual checking of credentials in all cases will be the sort of activity traditionally undertaken by professionals. If Carol's certificates are founded on checking the subject's passport, it may well be that the person who actually examines Alice's passport and issues her certificate is a clerk who has been trained in passport authentication, not an expert like a surveyor or valuer. There is no policy reason, however, why the classification of a certificate as a good or service should turn on whether the person making the report happens to be a professional. Furthermore, the certificate is not the only thing that the CA sells. In addition to the certificate and the investigatory services that it embodies, the CA also maintains (or contributes to) a CRL, without which a certificate is untrustworthy and thus of little or no value.[134]

Courts may, however, with some justice, view the CA's role as combining elements of provision of a service and the sale of a good. In such "mixed" cases, courts consider the applicability of Article 2 of the UCC to be a question of fact concerning the nature of the transaction. If the seller is providing a hybrid of a good and a service, the majority of states use a "predominant factor" test to determine whether Article 2 of the UCC should apply.[135] Under this test, the court attempts to determine the parties' intentions as to what was important. If the transaction is predominantly for the sale of goods, Article 2 of the UCC applies; otherwise it does not.[136] Other states either use a "final product" test which looks at what is left when a contract is completed,[137] or attempt to determine which classification best serves public policy.[138] As the courts have failed to achieve anything approaching uniformity in how they characterize the facts about

---

[134] *See supra* text accompanying notes 107-08.

[135] WHITE & SUMMERS, *supra* note 126, at 3-4.

[136] *Id.* at 3-4; *see also* Crystal L. Miller, Note, *The Goods/Services Dichotomy and the U.C.C.: Unweaving the Tangled Web*, 59 NOTRE DAME L. REV. 717, 720-23 (1984).

[137] Miller, *supra* note 136, at 726.

[138] *Id.* at 728-29.

mundane transactions,[139] it is entirely possible that courts in different jurisdictions will disagree about how best to characterize a CA's provision of certificates in the absence of legislation. Furthermore, some courts divide hybrid sales into the provision of a "good" and a "service" and then apply Article 2 of the UCC to the "goods" portion of the transaction.[140] CAs may be able to manipulate this characterization in some jurisdictions. For example, a CA that gives a client a certificate may be more likely considered to be selling a "good" than a CA that enters into a "service contract" by which the CA agrees to make the certificate available on a Web page to all who wish to see it.

The view that a CA is providing a service (or a hybrid in which the service element predominates) appears more convincing than the alternative under either the "predominant factor" test or the "final product" test.[141] Although it is true that a CA provides a "movable" thing to the client, that thing is digitized information[142] which is essentially useless without other supporting information provided by the CA on a continuing basis. To issue a certificate worthy of trust, the CA must: (1) have a valid and verifiable certificate of its own; (2) conduct the inquiry on which the certificate will be based; (3) accurately state facts in the certificate, including both the facts about the subject and the facts about the CA's investigation; and (4) maintain a CRL.[143] The CA's continuing duty to maintain the CRL in a form that can be

---

[139] *See* 1 RONALD A. ANDERSON, ANDERSON ON THE UNIFORM COMMERCIAL CODE § 2-105:51 (3d ed. 1981); Miller, *supra* note 136, at 717-20.

[140] *See* WHITE & SUMMERS, *supra* note 126, at 3-4.

[141] Whether this result best serves public policy is a difficult question, one which may become easier to answer once certificate-based electronic commerce becomes more commonplace and CAs have more of a track record.

[142] One issue in this context is whether that information is an "intangible" since it is generally but not universally agreed that Article 2 of the UCC does not apply to intangibles. Several writers have argued that the UCC should apply to software, even though it has properties that make it appear to be an "intangible." *See, e.g.*, Andrew Rodau, *Computer Software: Does Article 2 of the Uniform Commercial Code Apply?*, 35 EMORY L.J. 853 (1986); Bonna L. Horovitz, Note, *Computer Software as a Good Under the Uniform Commercial Code: Taking a Byte Out of the Intangibility Myth*, 65 B.U. L. REV. 129 (1985). Indeed, the courts that have spoken on this issue appear to be in general agreement that the UCC should apply to software. *See* Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1249 n.38 (1995) (noting that "most courts and commentators have concluded that distribution of mass-market software constitutes a sale of goods, thus invoking the UCC"). It could be argued that a certificate on a disk is more "tangible" than a certificate on a web site, but this privileges form over substance.

[143] ABA Draft Guidelines, *supra* note 4, § 3.11 cmt. 4.

rapidly and efficiently used by persons wishing to rely on a certificate is in itself significant evidence that the service element predominates in what the CA is selling. On the other hand, a CA which does no investigation at all and/or a CA that does not maintain a CRL may not be providing a "service." In that case, there is a real question whether the "good" being offered is fit and proper for its purpose.

Article 2 is being revised to extend its reach to "intangibles" such as computer software and data.[144] Thus, even if a certificate is outside the scope of Article 2 today, it does not necessarily follow that it will be outside the scope of Article 2 as ultimately revised. Nevertheless, so long as the revisions do not extend Article 2 to services, the argument that the service aspect of maintaining the CRL predominates over the sale of data as a "good" should remain valid.

A decision that a CA provides a service does not resolve all the ambiguities about a CA's liabilities in the absence of legislation, but it does provide a framework in which questions can be asked and answered. The next section briefly examines one of the ways in which a CA might face liability in the absence of a statute or other norms defining the rights and duties of a CA in order to demonstrate the legal complexities created by the introduction of a CA into a transaction. Of course, some scenarios are easy: if a CA is willfully or grossly negligent, or a CA conspires with the subject of the certificate, the CA should obviously be liable for its acts and omissions. Other scenarios, beyond the scope of this preliminary exploration, are not as straightforward. These include:

- The certificate is accurate, but the transaction goes wrong for some other reason.[145]

---

[144] *See* Nimmer, *supra* note 132.

[145] A CA should not be liable for the ways in which accurate certificates may be used by others. Both the Utah Digital Signature Act and the draft ABA Guidelines create a safe harbor from liability for a CA that has made accurate representations and complied with certain other requirements. *See, e.g.*, UTAH CODE ANN. § 46-3-304(4)(a) (providing for subscriber's indemnification of CA against claims due to subscriber's misrepresentation); *id.* § 46-3-309(2) (creating safe harbor against liability in excess of reliance limit stated in certificate for licensed CAs and limiting recovery in tort to compensatory damages). As a general matter, this makes sense: there is no reason why a CA should be involved in Alice's securities claim against Bob if the CA's only involvement was to provide accurate identifying certificates for the people involved. Of course, a different result would be appropriate if the CA provided an attesting certificate that was materially misleading. Different rules might arguably be appropriate for certain consumer transactions.

- The security of Alice's key is compromised and Mallet uses it, along with Alice's publicly available certificate, to impersonate Alice.[146]
- Alice revokes her key because she learns of Mallet's actions, but Mallet manages to transact during the period between Alice's revocation notice to Carol and Carol's posting of a certificate revocation.[147]
- The security of Carol's key is compromised and Mallet begins issuing bogus certificates or bogus certificate revocations.[148]
- Carol erroneously lists Alice's key as revoked, and Bob refuses to transact with Alice.[149]
- The "meltdown scenario": there is a major discovery in number theory or computation and the algorithms on which Alice and Carol's keys are based are no longer secure.

2. *Misrepresentation, Whether Wilful or Negligent, of CA's Client, Not Detected by CA*

Assume that Alice makes a negligent or wilful misrepresentation when procuring a certificate from Carol, a CA. The misrepresentation might be about Alice's identity, or her credit rating, or her employment. Carol fails to detect the misrepresentation. Alice then uses the certificate to transact with Bob, but either fails to pay or defrauds Bob in some manner. Assume further, for simplicity, that Bob can show that his reliance was reasonable,[150] that he would not have transacted with Alice but for her

---

[146] Unless Alice and Carol have made a special arrangement, a CA should have no duty to monitor the use of a certificate that they have agreed will be publicly available. Once notified of a key compromise, a CA should have a duty to publish this in the CRL "quickly." ABA Draft Guidelines, *supra* note 4, § 3.11 cmt. 4.

[147] Presumably the critical issue in this scenario will be whether Carol acted quickly enough. The common-law approach to this problem would rely on usages of trade, but it is difficult to do this when (1) there is as yet no "trade" to speak of, and (2) technology is changing very rapidly.

[148] Liability here may in part depend on how the key was compromised. There are differences between an inside job, penetration of Carol's systems by a hacker (perhaps due to bad security), an extraordinarily lucky brute force attack on Carol's key, advances in key-cracking technology (which raise the question whether these advances should have been anticipated), or Carol's failure to update her keys.

[149] This scenario resembles a bank dishonoring a check when there are sufficient funds in an account or a credit card clearer erroneously reporting that a credit limit has been exceeded or the card stolen.

[150] The degree to which Bob's reliance actually was reasonable may turn on a number of factors. One of the most important is the content of the certificate itself. If the certificate states that it should not be relied on for transactions over five dollars, Bob's reliance on the certificate for a $1 million transaction is unreasonable.

presentation of a verifiable certificate, and that the misrepresentation was material to the transaction.

If Carol made representations in the certificate as to the level of the inquiry used to verify Alice's claims about herself, the first issue is whether Carol should have detected Alice's misrepresentation given the promised level of inquiry. If Carol's practice statement proudly advertises that certificates are handed out to all comers, without any checking whatsoever, it is difficult to see how Carol could justly be accused of any form of negligence, assuming she accurately parroted Alice's claims, as long as it remains unreasonable to assume that all CAs conduct a minimum level of verification of their customers' assertions.[151] At this early stage in the development of certificate-backed electronic commerce, there are no usages of trade that might help define the standard of care that one might expect of a CA. There are, at present, no licensing or professional bodies whose standards could serve as the basis for a legal norm.[152] Perhaps some day CAs, like doctors and lawyers, will not be allowed to disclaim a minimum degree of investigation, or will only be allowed to disclaim after getting the client to acknowledge informed consent based on reading harrowing disclosures of the risks, but in the short term the representations contained in the certificate itself are likely to be the starting—and ending—point for defining the CA's duty to investigate.[153]

If, however, Carol claims that her certificates only go to people she has "thoroughly investigated,"[154] it may be reasonable to find that she was negligent in issuing the certificate containing the false information submitted by Alice. By asserting that she conducted an independent investigation, Carol negates any defense she may have as a mere republisher of Alice's statement.[155] And

---

[151] *But see supra* notes 141-43 and accompanying text (suggesting that CA who makes no representations as to service may be selling a "good" subject to UCC because no service is provided).

[152] A document such as the proposed ABA Digital Signature Guidelines, *see* ABA Draft Guidelines, *supra* note 4, may in time come to play this role.

[153] For a discussion of the similar problem of defining negligence in the absence of established usages of trade for Internet security professionals, see Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213, 243-52 (1995).

[154] *See supra* text accompanying note 37.

[155] Unless they have reason to know of the errors, publishers and book distributors are not liable for errors in works they publish and sell. *See, e.g.*, ALM v. Van Nostrand Reinhold Co., 480 N.E.2d 1263 (Ill. App. 1985) (dismissing negligence claim against publisher of allegedly unsafe "How To" book); Cardozo v. True, 342

if Bob has reasonably relied on Carol's certificate to his detriment, Carol may be liable to Bob under either contract or tort principles.[156]

a. Liability in Contract for Negligent Misstatements

Carol's potential contractual liability depends in part on with whom she has a contract. Carol's contract may be with Alice, the subject of the certificate, or it may be with another party, such as Alice's employer. But Carol does not have a contract with Bob, Alice's victim, who is the person most likely to sue. Nor does she have a contract with David, who was impersonated by Alice.

(i) Liability to Alice

If Alice benefited from Carol's error, she is unlikely to sue. If the error hurt Alice in some way, Alice's claim turns on Carol's failure to detect Alice's own error. In such cases, Alice's recovery is likely to be limited by her breach of contract in misinforming Carol. Even if Alice were able to persuade a court to grant her compensation, the measure of damages is likely to be restitution (that is, whatever Alice paid for the certificate) since she appears to have neither a reliance interest nor an expectation interest.[157]

(ii) Liability to Alice's Employer

Carol may have issued Alice's certificate at the request of Alice's employer, TED Corp. By failing to detect the falsity of Alice's claim that she was TED's Vice President in charge of purchasing when in fact she was a file clerk, Carol may have breached her contract with TED Corp. If Alice used the certificate in a way that harmed TED Corp, perhaps by buying tickets to Rio, TED Corp has a contract claim against Carol, although Carol again may have a partial defense of contributory negligence on the part of TED Corp's apparent agent, Alice, and possibly against anyone else at the company who may have corroborated her claims. Again, the measure of damages is likely

---

So. 2d 1053 (Fla. Dist. Ct. App.) (holding UCC did not make book dealer liable to purchaser of cookbook for lack of adequate warnings as to poisonous ingredients used in recipe), *cert. denied*, 353 So. 2d 674 (Fla. 1977).

156 Other remedies are available if Article 2 of the UCC applies. *See supra* part III.A.1.

157 *See* L.L. Fuller & William R. Perdue, Jr., *The Reliance Interest in Contract Damages*, 46 YALE L.J. 52 (1936) (defining three types of contractual interests).

to be restitution, since there is neither a reliance interest nor an expectation interest, although this time the amount of the contract may be somewhat larger.

(iii) Liability to Bob, Whom Alice Defrauded

Bob's hope of recovering under the contract between Carol and Alice (or Alice's employer) turns on his ability to characterize that contract as a third-party beneficiary contract of which he was an intended beneficiary.[158] Bob's ability to so characterize himself may also affect his right to recover in tort in states that adhere to a strong privity rule.[159]

Traditionally, Bob's hopes would have been slim. The first Restatement of Contracts divided third-party beneficiaries into three classes: "donee beneficiaries," "creditor beneficiaries" and "incidental beneficiaries."[160] Incidental beneficiaries have no contractual right against either party to the contract.[161] Bob is not a creditor beneficiary because the purpose of the contract between Alice and Carol is not to confer a gift on him. According to the first Restatement, Bob is a donee beneficiary when "it appears from the terms of the promise in view of the accompanying circumstances that the purpose of [Alice] in obtaining the promise . . . is . . . to confer upon [Bob] a right against [Carol]" that Bob would not otherwise have.[162] While it is certainly correct that Alice procured the certificate from Carol in order to show it to people like Bob and that this type of use was foreseeable, ordinarily there would be little reason to believe that Carol knew or should have known that Alice intended to show the certificate to Bob. In the era when privity reigned, Bob would not have been able to claim to be an intended beneficiary of the agreement without being specified as such when Alice procured the certificate.[163]

---

[158] *See* RESTATEMENT (SECOND) OF CONTRACTS § 302 (1979); David M. Summers, Note, *Third Party Beneficiaries and the Restatement (Second) Of Contracts*, 67 CORNELL L. REV. 880 (1982).

[159] *See* Gary Lawson & Tamara Mattison, *A Tale of Two Professions: The Third-Party Liability of Accountants and Attorneys for Negligent Misrepresentation*, 52 OHIO ST. L.J. 1309, 1319 (1991).

[160] *See* RESTATEMENT OF CONTRACTS § 133 (1932).

[161] *Id.* § 147.

[162] *Id.* § 133(1)(a).

[163] *See, e.g.*, Ultramares Corp. v. Touche, 174 N.E. 441, 445 (N.Y. 1931) (Cardozo, J.). Cardozo wrote:

> In the field of the law of contract . . . the remedy is narrower where the

Today, the picture is murkier.[164] "The *Restatement First* test, the intent-to-benefit test and its variations, and the *Restatement Second* tests are all inadequate and indeed largely meaningless."[165] Courts have relaxed the privity requirement in contract, as in tort,[166] replacing it with tests such as

> the balancing of various factors, among which are extent to which the transaction was intended to affect the [beneficiary], the foreseeability of harm to him, the degree of certainty that the [beneficiary] suffered injury, the closeness of the connection between the defendant's conduct and the injury, and the policy of preventing future harm.[167]

Nevertheless, courts remain reluctant to allow everyone be a potential third-party plaintiff in contract actions.[168]

Bob's position is not much clarified by the Restatement (Second) of Contracts, which provides that a third party may enforce a contract if he is an "intended beneficiary," that is, "if recognition of a right to performance in the beneficiary [Bob] is appropriate to effectuate the intention of the parties and . . . the circumstances indicate that the promisee [Alice] intends to give the beneficiary the benefit of the promised performance."[169] Whether the contract between Alice and Carol was for Bob's benefit or for Alice's depends entirely on how one chooses to

---

> beneficiaries of the promise are indeterminate or general. Something more must then appear than an intention that the promise shall redound to the benefit of the public or to that of a class of indefinite extension.

Id.; Moch Co. v. Rensselaer Water Co., 159 N.E. 896, 897 (N.Y. 1928) (Cardozo, J.); RESTATEMENT OF CONTRACTS § 145 (1932); *see also* RESTATEMENT OF CONTRACTS § 147 ("An incidental beneficiary acquires by virtue of the promise no right against the promisor or the promisee.").

[164] *See* Harry G. Prince, *Perfecting the Third Party Beneficiary Standing Rule Under Section 302 of the Restatement (Second) of Contracts*, 25 B.C. L. REV. 919 (1984) (summarizing wide variety of judicial responses to third-party benefit claims).

[165] Melvin A. Eisenberg, *Third-Party Beneficiaries*, 92 COLUM. L. REV. 1358, 1385 (1992).

[166] *See* William L. Prosser, *The Fall of the Citadel (Strict Liability to the Consumer)*, 50 MINN. L. REV. 791 (1966) [hereinafter *Fall of the Citadel*]; William L. Prosser, *The Assault Upon the Citadel (Strict Liability to the Consumer)*, 69 YALE L.J. 1099 (1960).

[167] Lucas v. Hamm, 364 P.2d 685, 687 (Cal. 1961) (citing Biakanja v. Irving, 320 P.2d 16, 19 (Cal. 1958)), *cert. denied*, 368 U.S. 987 (1962).

[168] *See e.g.*, Eisenberg, *supra* note 165, at 1374; Summers, *supra* note 158, at 893. Note that the breach by Alice of her contractual promise to tell the truth may not inevitably prevent recovery from Carol by a third party. *See* Lewis v. Benedict Coal Corp, 361 U.S. 459 (1960). *But see* RESTATEMENT (SECOND) OF CONTRACTS § 309(1)-(2); Eisenberg, *supra* note 165, at 1413 n.188.

[169] RESTATEMENT (SECOND) OF CONTRACTS, § 302(1). For a dissection of this section and its associated comments, see Eisenberg, *supra* note 165, at 1382-84.

look at it. Alice procures the certificate in order to induce Bob to transact with her. Alice wants Bob to rely on the certificate; perhaps Carol does also since this enhances the market for her product.[170] But Alice wants Bob to rely because it benefits her, not because it benefits him. The glass is either too empty or too full. Either the holder of the certificate, Alice, is the intended beneficiary because the certificate gives her something to show to Bob, or Bob is the intended beneficiary because without the benefit he will not transact with Alice.[171] Either no third party is intended or they all are.

(iv) Liability to David, Whom Alice Impersonated

Suppose that Alice persuades Carol to issue a certificate stating that Alice is David, an innocent third party. Alice then uses this certificate to defraud Bob, or just runs up a large number of debts she fails to pay. David may be justly aggrieved when a parade of unhappy Bobs comes to his door demanding payment. At the very least he will waste time straightening out the mess; his credit rating may be damaged; he may have to pay a lawyer. Like Bob, however, David's remedies, if any, are in tort. Indeed, David's contractual case is nonexistent since there is not even an argument that David was an intended beneficiary of the agreement.

b. Liability in Tort for Negligent Misrepresentation

Recovery in tort is generally premised either on the breach of a duty of care, or on strict liability.[172] Unlike their contract claims, the various parties' tort claims will in no way be undermined by any breach of contract Alice may have committed in misrepresenting facts to Carol, except of course for Alice, who

[170] Furthermore, the courts are not in agreement as to whether Alice's intent, Carol's intent, or their joint intent should control. *See* Jean F. Powers, *Expanded Liability and the Intent Requirement in Third Party Beneficiary Contracts*, 1993 UTAH L. REV. 67, 73-74.

[171] There is great merit to Professor Eisenberg's complaint that:

> the entire enterprise of finding an intent to benefit the third party as an end is misguided. Except in some cases involving true donee beneficiaries, the intent of the contracting parties is typically to further their own interests, not the interests of a third party. Accordingly, the question whether there is an intent to benefit the third party as an end normally cannot generate a meaningful answer.

Eisenberg, *supra* note 165, at 1381.

[172] *See infra* Part III.A.2.b(iv) (discussing imposition of strict liability on CAs).

may suffer from estoppel, unclean hands, or comparative fault. If Carol has a tort duty to issue accurate statements it exists outside the contract. Nevertheless, the contours of Carol's duty of care will, to a great extent, be defined by the representations she makes about the level of inquiry she promises to make before issuing a certificate. In a sense, therefore, the contract does define the tort;[173] anyone who relies on the certificate can reasonably be expected to take the trouble to read the terms incorporated into the certificate. For example, if Carol says in her certification practice statement, incorporated by reference in the certificate, that she requires applicants to show their passports, but in fact failed to ask Alice to show hers, she is guilty of negligence. Or, if Carol says that she checks passports, and did so, but failed to notice that Alice presented a crude forgery that could have been detected with ordinary care,[174] she is guilty of negligence. Conversely, if Carol did everything she said she would do, but Alice proffered a superbly faked passport, then Carol is not guilty of negligence. Bob and David may still be able to recover in this last case, however, if Carol is strictly liable for the accuracy of her certificates.[175] Even if Carol is not strictly liable, David may be such an attractive plaintiff that he stands to recover if his lawyer can find a way to get him to the jury.[176]

If Carol, the CA, breaches her duty of care in checking the facts about Alice recited in the certificate, she potentially is liable for making a negligent misrepresentation.[177] This liability may

---

[173] *Cf.* RESTATEMENT (SECOND) OF TORTS § 299A cmt. c (1965) ("In the ordinary case, the undertaking of one who renders services in the practice of a profession or trade is a matter of contract between the parties . . . .").

[174] The definition of "ordinary care" is itself an issue. If there is an industry, trade usages may supply a guide. *See supra* note 147. Otherwise, judges and juries will have to resort to general principles of ordinary care by reasonable people in like circumstances, whatever those may be.

[175] *See infra* Part III.A.2.b(iv) (discussing applicability of strict liability to CAs).

[176] Perhaps David's lawyer might accuse Carol of a privacy tort, or of casting David in a false light by identifying him with the evil Alice.

[177] The misrepresentation is clearly of a matter of fact, not opinion, as those terms are used in the RESTATEMENT (SECOND) OF TORTS, §§ 538A, 548A.

In some cases one could also hypothesize other claims against Carol, including false representation under 15 U.S.C. § 1125(a)(2) (1994) (trademark), which requires neither privity nor negligence, or a privacy tort. If Alice manages to acquire a certificate saying she is David, David may have a tort claim for appropriation of name or likeness, *see* RESTATEMENT (SECOND) OF TORTS § 652C ("One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."), or a false light claim against Carol, *id.* § 652E (publicity placing another in false light that is offensive, based on reasonable

run to Bob (Alice's victim), to David (if Alice impersonated him), to Alice's employer (if the certificate was pursuant to a contract with the employer) and perhaps even to Alice, subject to her contributory or comparative negligence or unclean hands if she committed a fraud.[178]

A threshold issue, however, is to whom the negligent misrepresentation in the certificate is addressed. If Bob got his copy of the certificate from Carol's Web site where she publishes certificates, Bob has a tort claim for a negligent misrepresentation that Carol made directly to him, although contract privity is absent.[179] David cannot make this claim—he is a third party and his ability to recover depends on how the applicable state's law treats third parties claiming injury from negligent misrepresentation to another. On the other hand, if Carol gives the certificate to Alice and Alice sends a copy of it to Bob, the negligent misrepresentation was made to Alice and Bob is reduced to a third party.

States differ greatly on when a third party can obtain redress for negligent misrepresentations.[180] Some require only that the third party's reliance be foreseeable; most follow the Restatement (Second) of Torts rule which is an uneasy, and sometimes unclear, compromise between the two views; a few require contract privity.

(i) Foreseeability States

A small, but perhaps growing,[181] number of states determine who may bring a third party negligent misrepresentation claim by applying traditional tort analysis focusing on foreseeability. Carol clearly would be liable to Bob in these states, regardless of how he obtained the certificate, since it is completely foreseeable that persons such as Bob would rely on the certificate. Carol should be liable to David as well, since it is foreseeable that a person whose good name is misappropriated in a certificate will

person standard, subjects publisher to liability if published with knowledge of or reckless disregard as to falsity), or perhaps even a new tort of impersonation.

[178] *See* 9 STUART M. SPEISER, ET AL., THE AMERICAN LAW OF TORTS §32:74, at 367 (1992).

[179] There may be interesting choice of law problems if Carol and Bob live in different jurisdictions.

[180] *See generally* Jordan H. Leibman & Anne S. Kelly, *Accountants' Liability to Third Parties for Negligent Misrepresentation: The Search for a New Limiting Principle*, 30 AM. BUS. L.J. 347 (1992).

[181] James R. Adams, *No Privity Required for Negligent Misrepresentation Action*, 60 DEF. COUNS. J. 601 (1993).

be harmed. Both the equities and an economic analysis favor David since he is completely innocent, had no notice, and there is nothing he could have done to protect himself from Alice.

(ii) Restatement States

Most states follow the rule set out in section 552 of the Restatement (Second) of Torts[182] and allow a third party to sue if he is within the group of actually foreseen (not all foreseeable) users, the "limited group of persons for whose benefit and guidance" to whom the author knows the "recipient intends to supply" the statement.[183] Unfortunately, the Restatement rule is difficult to apply to a CA. The potential class of persons who will be shown a certificate and asked to rely on it is large, much like an appraiser's or accountant's report. Indeed, the potential class is as large or larger than those who might rely on a report regarding a publicly traded security; the possible transactions are more diverse and the reliance by the third party is more likely to be a "but for" element of the transaction. Furthermore, any CA must be aware of these facts. Because the whole point of having a certificate is to enable the holder to show it to someone who will rely on it, there is no question that the recipient of a valid and verifiable certificate should be within the zone of foreseeable users, that is, among those entitled to "justifiable reliance."[184]

---

[182] *See, e.g.*, Bily v. Arthur Young & Co., 834 P.2d 745, 773 (Cal. 1992) (adopting RESTATEMENT (SECOND) OF TORTS § 552 approach). The relevant part of section 552 states:

> (1) One who, in the course of his business, profession or employment, or in any other transaction in which he has a pecuniary interest, supplies false information for the guidance of others in their business transactions, is subject to liability for pecuniary loss caused to them by their justifiable reliance upon the information, if he fails to exercise reasonable care or competence in obtaining or communicating the information.
>
> (2) Except as stated in Subsection (3), the liability stated in Subsection (1) is limited to loss suffered
>
> (a) by the person or one of a limited group of persons for whose benefit and guidance he intends to supply the information or knows that the recipient intends to supply it; and
>
> (b) through reliance upon it in a transaction that he intends the information to influence or knows that the recipient so intends or in a substantially similar transaction.

RESTATEMENT (SECOND) OF TORTS § 552.

[183] RESTATEMENT (SECOND) OF TORTS § 552(2)(a); *see, e.g.*, Rosenblum Inc. v. Adler, 461 A.2d 138, 145 (N.J. 1983).

[184] *Arthur Young & Co.*, 834 P.2d at 772.

The problem with this line of reasoning, however, is that it seems to prove too much. While section 552 of the Restatement (Second) is not a model of clarity, it is a compromise that was not intended to expand the class of potential third-party plaintiffs to the entire world.[185] The class of potential users of a certificate is all users of electronic commerce, indeed all users of e-mail or the World Wide Web, which may equal a good fraction of the world someday; allowing a right of action to this entire group threatens to collapse into the foreseeability test, and thus to exceed the boundaries that section 552 was designed to create. There has been a trend toward allowing third parties to assert negligent misrepresentation claims against professionals, but this trend has not been uniform across states, nor even across professions within individual states.[186] Some have argued that professional opinions such as audits are intended primarily for the benefit of third parties and that accountants should therefore be liable to these essentially foreseeable parties,[187] but many others strongly oppose this idea.[188] Part of this debate concerns the extent to which accountants can foresee the uses to which their clients will put their work product, but commentators have also argued that unfettered liability is disproportionate to the wrong, might discourage socially useful behavior (such as audits of litigation-prone industries), might be expensive to administer, or might otherwise impose greater social costs than benefits.[189]

The CAs' circumstances are materially different from the accountants' in one important respect. If Bob acquires a certificate from Alice, that certificate has almost no value to Bob except as a means of facilitating transactions with other parties.[190] *Every*

185 *See* RESTATEMENT (SECOND) OF TORTS § 552 cmt. a (noting that liability for negligent misstatement is more restricted than for fraudulent misrepresentation).

186 *See* Lawson & Mattison, *supra* note 159, at 1310.

187 *See, e.g.*, Howard B. Wiener, *Common Law Liability of the Certified Public Accountant for Negligent Misrepresentation*, 20 SAN DIEGO L. REV. 233, 250 (1983); Richard D. Holahan, Jr., Note, Security Pacific Business Credit, Inc. v. Peat Marwick Main & Co.: *Just in Case You Had Any Doubts—There Is No Tort of Negligent Misrepresentation in New York*, 13 PACE L. REV. 763, 771-76 (1993).

188 *See, e.g.*, Victor P. Goldberg, *Accountable Accountants: Is Third-Party Liability Necessary?*, 17 J. LEGAL STUD. 295 (1988); Thomas L. Gossman, *The Fallacy of Expanding Accountants' Liability*, 1988 COLUM. BUS. L. REV. 213; John A. Siliciano, *Negligent Accounting and the Limits of Instrumental Tort Reform*, 86 MICH. L. REV. 1929 (1988).

189 *See, e.g.*, Siliciano, *supra* note 188, at 1944.

190 The picture is somewhat more complicated if Alice's employer obtains the certificate for Alice, since the certificate may have uses within the organization.

recipient of a certificate who suffers because of the CA's negligence thus falls squarely within the Restatement (Second) section 552 class of persons who suffer loss "through reliance upon [the negligent misrepresentation] in a transaction that [the CA] intends the information to influence or knows that the recipient so intends or in a substantially similar transaction."[191] It may be that the CA's resulting liability is unfairly large or socially detrimental, but it is hardly incidental or unexpected.

(iii) Privity States

A few states, notably New York, still follow the older rule that if Bob is a third party he can only recover for Carol's negligent misrepresentation to Alice (that Alice then furnished to him) if he is in a relation of privity with Carol, although some of these states slightly relax the qualifications for privity.[192] The policy reason for attempting to limit the class of potential plaintiffs claiming negligent misrepresentation is in deference to what are considered to be legitimate fears of indeterminate liability to third persons. In the infamous words of Justice Cardozo in *Ultramares Corporation v. Touche*, "If liability for negligence exists, a thoughtless slip or blunder, the failure to detect a theft or forgery beneath the cover of deceptive entries, may expose accountants to a liability in an indeterminate amount for an indeterminate time to an indeterminate class."[193]

The classic cases about negligent misrepresentation, such as *Ultramares*, involve a common fact pattern in which Bob receives Carol's negligent misrepresentation (regarding, for example, an accountant's report) from Alice. If Bob got the certificate from Alice, his third party negligent misrepresentation claim hews closely to the *Ultramares* facts, giving Bob little hope of recovery against Carol in a privity state.

Bob's position in a privity state such as New York is more complicated if he got Alice's certificate directly from Carol's Web site. It is as if the accountants in *Ultramares* had published the accounts to the world with their client's consent. Yet, Bob still

---

[191] RESTATEMENT (SECOND) OF TORTS §552(2)(b). Arguably these third parties are thus within the "limited group of persons for whose benefit and guidance [Alice] intends to supply the information or knows that the recipient intends to supply it," *id.* § 552(2)(a), even if this "limited group" is in fact limited only to those with computers.

[192] *See* 9 SPEISER, *supra* note 178, § 32:75, at 370.

[193] Ultramares Corp. v. Touche, 174 N.E. 441, 444 (N.Y. 1931).

has no contract privity with Carol. As a formal matter, staying squarely within the language of *Ultramares*, Bob's claim is unchanged. Nor does the direct provision of the certificate have any formal effect on Bob's status as a potential third-party beneficiary of the contract—a status that would substitute for privity[194]—since Carol and Alice's intentions are a necessary element of Bob's third-party beneficiary contract claim,[195] and their intentions are not affected by the mode of delivery.

Carol's claim that she did not foresee Bob's reliance rings particularly hollow if she placed Alice's certificate on the World Wide Web herself rather than giving it to Alice; Bob's claim of justifiable reliance on a certificate published by Carol in this manner seems strong. Nevertheless, since a certificate issued by Carol is used, foreseeably, by the same people in the same way for the same purposes regardless of whether it happens to pass through Alice's hands on the way to Bob, it seems overly formalistic to make a distinction between the legal consequences of the two distribution models. Indeed, with the exception of the case where Alice notifies Carol that she intends to give Bob the certificate, Bob is just as much—or as little—an intended third party beneficiary whether Alice publishes the certificate or Carol does. Because in practice the two distribution methods are barely distinguishable, especially when one considers that Carol continues to manage the CRL regardless of who distributes the certificate, there is a danger that Bob's tort claim would fail in a strong privity state such as New York even if he got Alice's certificate directly from Carol.[196]

Whatever this result may say about general tort principles applicable in New York, it is not a sensible result in the special context of a CA who issues a certificate at the request of a client, particularly if the CA publishes the certificate. The rule in *Ultramares* was crafted to protect accountants and other professionals from being subjected to unforeseen, arguably unforesee-

---

194 *See* Lawson & Mattison, *supra* note 159, at 1319.

195 *See supra* note 169 and accompanying text.

196 *Cf.* Holahan, *supra* note 187. A CA that wanted to take on liability in such a state in order to signal that its certificates were reliable would either have to draft a contract that made its intentions very clear, or it might have to adopt a business model in which Carol does not put Alice's certificate on a web page, and does not make it available to all, but instead provides an automated e-mail credential response service in which Carol meters Alice's usage of the certificate, and perhaps charges accordingly.

able, liability by the actions of a client in cases where the person issuing a report could reasonably believe that the report was for the client's own, private, use.[197] A CA issuing a certificate, especially an identifying certificate, knows full well that the client's entire purpose in acquiring the certificate is to show it to third parties who will rely on it. By publishing the certificate itself, the CA removes itself from the *Ultramares* facts. Even if the client publishes the certificate, the CA must logically know that the client intends to do so. The CA cannot, therefore, credibly claim surprise when an unknown third party relies on the certificate in a manner consistent with the CA's representations in that certificate because the certificate exists solely to be relied upon by strangers. The common law should reflect this reality, particularly in the case where the CA itself is the publisher, even in a strong privity state.

(iv) Strict Liability for CAs?

Strict liability is most commonly applied in cases involving goods, such as defective products, and ultrahazardous activities. Furthermore, strict liability traditionally allows recovery for personal injury but not for "economic loss." Traditionally, strict liability would thus seem to have had little to do with the issuance of certificates: they are not ultrahazardous in the usual sense of the term,[198] and they are probably not "products."[199] However, one commentator suggests that a certificate which used a faulty algorithm to produce the CA's digital signature might be found to have a design defect.[200] Given that some jurisdictions separate "hybrid" good-service transactions into the part that is a good and the part that is a service,[201] it may be useful to consider briefly the economic principles that might underlie the imposition of strict liability as they apply to certificates as "goods." Indeed, there is a policy argument that a regulatory approach to the law of certification authorities might want to take these factors into account in assigning liability, particularly in the absence

---

[197] *See supra* note 193 and accompanying text.

[198] *But see supra* text at notes 120-21 (discussing proposals to make consumers presumptively liable for all transactions with their digital signature supported by valid certificate).

[199] *See supra* text accompanying notes 133-34 (making the argument that certificate is not a "good" for UCC purposes).

[200] BAUM, *supra* note 22, at 130-31.

[201] *See supra* note 140 and accompanying text.

of the consensus as to what constitutes due care for a CA needed to give teeth to the CA's duty of care.

Imposition of a strict liability regime eliminates the need to find privity: liability follows the good.[202] There is no requirement that plaintiff show fault by defendant; instead, the sole issue is whether the product performed adequately. The Restatement (Second) of Torts section 402A imposes strict liability on products with an unreasonably dangerous defect.[203] Prosser defined this class of products as those which are "not safe for such a use that can be expected to be made of [them], and no warning is given."[204]

The Learned Hand test, as reformulated by Dean Calabresi, suggests that courts should impose strict liability on the least-cost avoider.[205] As between Carol and anyone but Alice, Carol will in most cases be the least-cost avoider of the loss caused by an inaccurate certificate. If Alice and Bob are strangers, Bob has no means of testing the validity of the representations in the certificate: his inability to confirm Alice's claims about herself is the precise reason he wants the certificate in the first place.[206] As between Carol and Alice, however, Alice is ordinarily the least-cost avoider of Alice's errors.

The net effect of a policy that makes Alice strictly liable to everyone for her own errors in a certificate, and makes the CA strictly liable to everyone but Alice for the CA's failure to detect Alice's misstatements, would be to turn the CA into an insurer for Alice's veracity in every case where Alice disappears or lacks the assets to satisfy a judgment.[207] There is also a danger that imposing strict liability on Carol removes the incentive for Alice to take care that her statements to Carol are accurate. For Carol to agree to be a CA under these terms would require that Alice provide either extraordinarily strong assurances as to her claims,

---

[202] *See* MacPherson v. Buick Motor Co., 111 N.E. 1050 (N.Y. 1916).

[203] RESTATEMENT (SECOND) OF TORTS § 402A, cmt. i (1977) (discussing definition of "unreasonably dangerous").

[204] Prosser, *Fall of the Citadel*, *supra* note 166, at 826.

[205] *See* GUIDO CALABRESI, THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS (1970); Guido Calabresi & Jon T. Hirschoff, *Toward a Test for Strict Liability in Torts*, 81 YALE L.J. 1055, 1077 (1972).

[206] *See generally* Part I *supra*.

[207] There is also some danger that under a strict liability regime, the fact that Carol was willing to become an insurer for Alice might itself be a signal that Carol was not trustworthy.

or that Carol charge prices large enough to pay for a generous insurance cover.

B. Contractual Attempts to Limit Private CA Liability

Even absent strict liability, the current uncertainty as to the state of the law gives a CA an incentive to be overcautious. A lawyer retained by a CA is likely to respond by attempting to have the CA disclaim any responsibility for anything it says. Thus, for example, the disclaimer offered by an early entrant to this market, in its standard contract with purchasers of certificates entitling them to run a Netscape-compliant "secure server," states:

> VERISIGN DISCLAIMS ANY WARRANTIES WITH RESPECT TO THE SERVICES PROVIDED BY VERISIGN HEREUNDER INCLUDING WITHOUT LIMITATION ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. VERISIGN MAKES NO REPRESENTATION OR WARRANTY THAT ANY CA OR USER TO WHICH IT HAS ISSUED A DIGITAL ID IN THE VERISIGN SECURE SERVER HIERARCHY IS IN FACT THE PERSON OR ORGANIZATION IT CLAIMS TO BE WITH RESPECT TO THE INFORMATION SUPPLIED TO VERISIGN. VERISIGN MAKES NO ASSURANCES OF THE ACCURACY, AUTHENTICITY, INTEGRITY, OR RELIABILITY OF INFORMATION CONTAINED IN DIGITAL IDS OR IN CRLs COMPILED, PUBLISHED OR DISSEMINATED BY VERISIGN, OR OF THE RESULTS OF CRYPTOGRAPHIC METHODS IMPLEMENTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY VERISIGN OR ITS EMPLOYEES OR REPRESENTATIVES SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF VERISIGN'S OBLIGATIONS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.[208]

Leaving aside the issue of the enforceability of this language, especially as applied to third parties,[209] if Carol in fact "makes no

---

[208] VeriSign Corp., Secure Server Legal Agreement 3, *available online* URL http://www.verisign.com/netscape/legal.html.

[209] In California, where VeriSign is located, the disclaimer will not work if a certificate is a good because an "as is" disclaimer or one which disclaims "all implied warranties that would otherwise attach to the sale of consumer goods under the provisions of this chapter," CAL. CIV. CODE § 1791.3 (West 1985), must be "a conspicuous writing . . . attached to the goods." *Id.* § 1792.4(a). It is unclear how one

representation or warranty" that the holder of one of her identifying certificates "is in fact the person or organization it claims to be with respect to the information supplied to" Carol, and if she also disclaims "the accuracy, authenticity, integrity, or reliability of information" the certificate provides, one is entitled to ask how much point there is to having one of Carol's certificates.[210] The answer depends primarily on what Alice and Bob decide they need in order to feel comfortable transacting with each other. If a certificate provides transactional confidence, at least in the absence of alternatives, then it suffices. Carol's desire to protect her service's reputation may, in any case, provide Alice and Bob with some comfort that Carol has been verifying the accuracy of Alice's assertions.

Similarly, because the law today offers a CA no obvious means of pegging its liability according to the degree of investigation that went into a certificate, a CA in operation today may seek to reduce its liability to the minimum. Again, VeriSign provides an example in its standard contract:

> NEITHER PARTY WILL BE LIABLE TO THE OTHER FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL OR INCIDENTAL DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE, ARISING OUT OF BREACH OF ANY EXPRESS OR IMPLIED WARRANTY, BREACH OF CONTRACT, MISREPRESENTATION, NEGLIGENCE, STRICT LIABILITY IN TORT OR OTHERWISE, EXCEPT ONLY IN THE CASE OF WILLFUL MISCONDUCT, DEATH OR PERSONAL INJURY WHERE AND TO THE EXTENT THAT APPLICABLE LAW REQUIRES SUCH LIABILITY. THE PARTIES AGREE THAT VERISIGN'S TOTAL LIABILITY HEREUNDER SHALL NOT EXCEED THE AMOUNTS PAID BY CUSTOMER TO VERISIGN UNDER THIS AGREE-

---

achieves this for a certificate. For a survey of limits on disclaimers in the U.S. see Donald F. Clifford, Jr., NON-UCC STATUTORY PROVISIONS AFFECTING WARRANTY DISCLAIMERS AND REMEDIES IN SALES OF GOODS, 71 N.C. L. REV. 1011 (1993).

[210] Indeed, one can imagine a court throwing out the disclaimers as unconscionable. *See* U.C.C. § 2-302; *see also id.* at cmt. 1 (suggesting courts should strike as unconscionable clauses "contrary to public policy or to the dominant purpose of the contract"). This section has been applied to many kinds of contracts other than those for goods "either by analogy or as an expression of a general doctrine." E. ALLAN FARNSWORTH, CONTRACTS § 4.28, at 325 (2d ed. 1990); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 208 (1979); CAL. CIV. CODE § 1670.5 (West 1985). *Compare* Wile v. Southwestern Bell Tel. Co., 549 P.2d 903 (Kan. 1976) (finding disclaimers of liability for error in telephone book not unconscionable) *with* Allen v. Michigan Bell Tel. Co., 232 N.W.2d 302 (Mich. Ct. App. 1975) (finding disclaimers for errors in telephone book to be unconscionable).

> MENT EXCEPT TO THE EXTENT THAT SUCH LIABILITY AROSE FROM VERISIGN'S WILLFUL MISCONDUCT. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.[211]

With this disclaimer, the CA seeks to limit its liability to its client for anything other than its own "willful misconduct" to the amount the subscriber paid for the certificate, which is likely to be a very small sum in most cases. The desire to limit liability in this manner is a response to the largely unpredictable and potentially capacious liability that a CA might encounter in the absence of a statute or other norms defining its rights and duties. Unfortunately, this response threatens to undermine the certificate itself. A certificate that contains a warning that it is not to be trusted seems ill-suited to fill a trust-building role in electronic commerce. A world in which such warnings are routinely given and routinely ignored suggests that at least one party's expectations will be disappointed.

C. Is CA Legislation Needed to Resolve Liability for an Erroneous Certificate?

A CA's fundamental duty, whether in contract or tort, should be to make accurate representations in a certificate. In a certificate worthy of reliance, these representations will concern not only facts about the subject of the certificate, but also facts about the CA itself. To inspire confidence, a certificate should state (or incorporate by reference) the identity of the CA, the facts upon which the identification of the subject of the certificate is based, the degree of investigation performed by the CA to confirm the facts stated by the subject of the certificate, the start and end dates of the certificate's validity and the location of the relevant CRL. CAs might choose to include additional information, such as a recommended reliance limit for transactions based on the certificate.

One can imagine that as the number of CAs grows, certificates will eventually begin to be issued that bear all the indicia of reliability through the operation of market mechanisms. This is an uncertain process, however, and it is not instantaneous. Further-

---

211 VeriSign Corp., *supra* note 208, at 3.

more, the existing uncertainty about the substantive law applicable to CAs increases the risk involved in running one. All other things being equal, this will raise the cost of certificates, as risk-averse parties may be unwilling to enter the market, reducing the number of competitors:

1. The Case for Legislation

The case for legislation begins with the observation that the legal climate for CAs is uncertain. Uncertainty increases costs and discourages transactions.[212] In the case of CAs it threatens to produce overpowerful incentives for CAs to underproduce certificates and/or disclaim all liability for certificates, which threatens to limit their utility.[213] It is also likely to lead to considerable litigation until all the relevant rules are identified.

As we have seen, absent legislation a CA's liability is potentially high. Much of the social benefit of having a certificate-based system of electronic commerce is foregone if Carol's exposure to liability is so high that the cost of insurance is enormous. In that case Carol will self-insure, and declare bankruptcy if a large claim is decided against her, which does not help the injured parties and creates a risk that CAs will not last. Alternately, Carol will have to charge high prices and issue few certificates, which also defeats the purpose of the system.

A CA's liability can be fixed by legislation, but this requires a policy choice as to what the appropriate level of liability should be. The Utah Act provides one model. Under that Act, a CA that complies with relatively onerous requirements[214] is granted a safe harbor from consequential damages, and indeed from most liability in excess of a reliance limit stated in the certificate, even if the CA itself is guilty of a negligent misstatement.[215] It is certainly possible to imagine other levels at which the CA's liability

---

[212] *See generally* Karl N. Llewellyn, *Why We Need the Uniform Commercial Code*, 10 U. FLA. L. REV. 367 (1957).

[213] However, the existence of standards such as X.509 impose significant constraints on CA behavior. For example, to comply with X.509 a CA must uniquely identify itself in a certificate. *See* Ford, *supra* note 23, at 12. Failure to produce a certificate that complies with the standard designed into systems that use certificates will result in users rejecting the certificate.

[214] These requirements include: having a secure system, trusted personnel, clear certification policies, insurance, a CRL, a certificate from the root CA operated by the state, regular financial audits of its balance sheet, and regular security audits of its computer systems. UTAH CODE ANN. § 46-3-201, -202, -203, -301, -307.

[215] The Utah Act states that a CA which complies with its terms is:

might be fixed in the event that it is negligent, levels which create an additional incentive to be careful but fall short of open-ended liability.[216]

Another reason legislation might be needed is to make provisions for certificates issued by a CA that later goes out of business. A CA cannot recall all of its certificates; a bankrupt CA might have no incentive to even notify its former clients that it was ceasing operations. Some certificates, particularly transactional certificates, may be on documents with a long lifespan. The need to check the validity of the digital signatures on a deed may not arise until many years after it is affixed, but the need is no less real. If the CA is to go out of business in a manner that does not undermine the utility of such certificates, someone must be found to store the certificates that validate the CA's key and to take over the management of the CA's CRL, without which all of its certificates must be considered unreliable.[217]

Legislation may also serve the goal of consumer protection (depending on its content), since a statute can require that CAs carry insurance or reserves to meet any claims for their errors. CAs resemble notaries public in that both verify the authenticity of signatures, and it may follow that, like notaries, CAs "require some level of licensing by governmental entities" to ensure public confidence.[218]

B. not liable in excess of the amount specified in the certificate as its recommended reliance limit for either:
   (I) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or
   (II) failure to comply with [rules relating to the proper issuance of a certificate] in issuing the certificate;
C. liable only for direct, compensatory damages in any action to recover a loss due to reliance on the certificate, which damages do not include:
   (I) punitive or exemplary damages;
   (II) damages for lost profits, savings, or opportunity; or
   (III) damages for pain or suffering.

Id. § 46-3-309(2).

[216] On the other hand, once the decision to have comprehensive legislation has been made, the case seems overwhelming for reemphasizing that a CA should never be liable for anyone's use of an accurate certificate that the CA had no reason to suspect was no longer accurate—even if this is certain to be the common-law result absent legislation.

[217] Utah addresses these issues in its administrative rules issued pursuant to Section 104 of the Utah Digital Signature Act. *See id.* § 46-3-104(3).

[218] Henry H. Perritt, Jr., *Access to the National Information Infrastructure*, 30 WAKE FOREST L. REV. 51, 100 (1995). On the other hand, equal public confidence might be achieved by clear legal rules which either impose liability on CAs for their

A single standard should also prevent the duplicative litigation that would otherwise be required to identify the relevant rules in many jurisdictions. Furthermore, the likelihood that different jurisdictions will have different liability rules reduces the utility and ease of use of certificates. Without new laws, uniformity among states, much less among nations, is unlikely. The American Bar Association is working on Guidelines for Digital Signatures,[219] and the Commissioners on Uniform Laws are studying the issue.

While the liability and uncertainty arguments have power, the strongest argument for legislation is that it would create an opportunity to standardize the rights and duties of CAs, their customers, and those who rely on certificates, regardless of the jurisdiction in which they happen to reside. It is possible to imagine a system in which users grade certificates according to the liability regime that applies, but it seems unwieldy and inefficient to force users (or their software) to take account of factors such as the effect of the geographical location of the CA and the trading parties on the choice of law. This is especially true when information about geographical location may not necessarily be accessible to participants in Internet commerce.[220] Users cannot reasonably be expected to keep abreast of changes in the law of multiple jurisdictions, and the challenge of programming a certificate system to do more than classify certificates by their reliance limits seems daunting. One can imagine the introduction of yet another intermediary that would perform this rating function, but requiring the introduction of a trusted fourth party to rate trusted third parties seems to be too much of a good thing. A uniform national or even international rule would be much easier to understand and to administer.

2. *The Case Against Legislation*

The case against new legislation is that it would be too much too soon, and perhaps too unfair. First, although the idea of a CA is not new, commercial CAs are so new that the industry barely deserves to be called a fledgling. At this stage, with few providers, few clients, and few certificates, it is difficult to foresee how certificates will actually be used with sufficient precision to

errors or at least make it possible for CAs to signal their confidence in their certificates by undertaking a measured amount of liability.

[219] *See* ABA Draft Guidelines, *supra* note 4.

[220] *See generally* Froomkin, *supra* note 21.

draft rules that will last. Any statute written today, including the Utah Act, is a first draft. Second, it is at least conceivable that the marketplace will provide an adequate solution without regulation. If a competitive market in certificates arises, it is possible that a struggle to the top[221] (or market stratification) may ensue, and that CAs may find that a willingness to back their certificates with at least some kind of guarantee may make their certificates more attractive to clients and third parties.[222]

The clients' interests depend in large part on how they plan to use the certificate. If Alice plans to use the certificate to transact with Bob, Alice wants the least expensive certificate that Bob will find acceptable.[223] Bob, on the other hand, may want a certificate that gives him recourse against the CA if Alice succeeds in defrauding him and turns out to be an imposter. Similarly, Alice's demands regarding the assurances she wants to receive about Bob will play a large role in the level of assurance Bob will want to be able to display. In other words, neither Alice's nor Bob's interests are necessarily well served by a world in which CAs have no liability to either of them under any circumstances. The CA itself may benefit from a regime in which it at least has the option of taking on liability to demonstrate its confidence in the certificates. Although the Utah Act allows CAs to take on additional liability if they want, market pressures arguably may produce optimal outcomes without regulation.

Even if Carol says that her Class A certificates are not suitable to transactions of more than five cents, Alice may be able to use the certificate millions of times in an hour. It might, however, be possible for Carol to say that Class A certificates are only suitable for transactions of five cents or less *and* that each individual third party may rely on a certificate only once per day. This would impose an additional, but perhaps not unreasonable, recordkeeping obligation on Bob since now he has to make sure that Alice has not used the certificate with him that day. Bob is of course free to dispense with this recordkeeping, but if he does so he bears the risk that the certificate is erroneous because his

---

221 *See generally* Ralph K. Winter, Jr., *State Law, Shareholder Protection, and the Theory of the Corporation*, 6 J. LEGAL STUD. 251 (1977).

222 The Utah Act allows CAs to take on additional obligations to clients or others if they so desire. UTAH CODE ANN. § 46-3-302(3).

223 If Alice plans to transact with many people, she will have to trade the expense of the certificate against the likelihood that it will be accepted by those with whom she wishes to transact.

reliance on the certificate in excess of its terms is not justified. Even if such a scheme were feasible, it would only protect Bob against overreliance on a once-a-day certificate. It would not protect Alice against Mallet's misuse of her signature if he gained control of it. Because a digital signature supported by a valid certificate can be used to transact with a very large number of people in a short period of time, only usage monitoring by the CA itself, or by the CA's agent managing a unique CRL, could turn the reliance limit into an effective protection against multiple use. Unfortunately, there is reason to doubt whether it is technically and economically feasible for a CA to do this;[224] there has been no suggestion that any potential CA is interested in shouldering this substantial burden.

Utah's approach to the CA liability question creates two categories of CAs. Those that comply with the relatively strict requirements of the Utah Act by proving their technical and financial security can benefit from a very safe harbor from liability for erroneous certificates.[225] Noncomplying CAs are left to the tender mercies of the background law. The commentary to the Utah law notes that CA liability limits are justified because "one of the principal impediments to the emergence of certification authorities has been the uncertainty of the legal risks such a business would undertake."[226] Indeed, when the Utah Act was enacted in early 1995, there were no commercial CAs offering certificates to the public in the United States, nor were there any as of February 1, 1996.

By early 1996, however, Netscape 2.x browsers came equipped to recognize certificates issued by CommerceNet, MCI Mall, ATT, RSA, and Netscape.[227] Although at this writing these entities have yet to begin issuing certificates on a large scale, it seems plausible that they will do so even in the absence of legislation. If they do begin issuing certificates on a large scale in the absence

---

[224] One of several obstacles to any system that seeks to count the number of uses of a certificate is that both certificate lists and CRLs are easily copied. If Bob runs a high-volume, low-margin business, in many cases it will be far more efficient for him to copy an entire CRL at random intervals, and take the risk of honoring a revoked certificate from time to time, than to continually contact the CA to check individual certificates.

[225] *See* UTAH CODE ANN. § 46-3-309.

[226] *Id.*, cmt. a, *available online* URL www.state.ut.us/ccjj/digsig/dsnt-act.htm.

[227] Netscape 2.01, Options menu, Security Preferences menu, Site Certificates menu; *see generally* Netscape Handbook: Application Features, *available online* URL http://home.netscape.com/eng/mozilla/2.01/handbook/docs/appans.html#C37.

of legislation, the argument that they require substantial protection from liability in order to enter the market will be at least weakened, and perhaps even proved wrong. "Perhaps" is, however, the strongest word appropriate at this time. The willingness of large organizations to enter the market in advance of legislation that they may reasonably expect will provide liability shields does not necessarily prove that they would remain willing to issue certificates if it became clear that the legislation was not going to materialize. Some CAs may choose to take a calculated short-term risk to expose themselves to high liability in order to grab market share and create brand name recognition. These same CAs might be unwilling to shoulder the risk in the long term. Nevertheless, to an opponent of legislation, "perhaps" is good enough since the crux of the argument is that one should wait and see.

Similarly, the opponent of legislation is unlikely to be fazed by the preliminary evidence that fear of liability has forced one CA to include scattershot disclaimers in its certificates.[228] Even if one agrees that if this practice persisted it would risk undermining the utility of certificates, there is arguably little to be gained by legislating before the market for certificate policies has had an opportunity to reach equilibrium.[229]

Finally, if the market requires standardized rules, the competition between states may provide them without federal assistance, as demonstrated by the predominant role of Delaware's corporate law.[230] Perhaps Utah, or some other state, or even a foreign country, will become the address of choice for CAs that wish to signal their trustworthiness.

3. *The ABA Digital Signature Guidelines*

One of the difficulties in determining the duties and liabilities of CAs in the absence of legislation is the paucity of trade practices or best practices.[231] A further difficulty is that lawyers and judges are generally unfamiliar with the purpose and functions of digital signatures and CAs. The ABA Section on Science and

---

[228] *See supra* note 211 and accompanying text.

[229] A supporter of legislation would be likely to counter that the process of finding this equilibrium would requires enormous amounts of wasteful litigation.

[230] *Cf.* Roberta Romano, *Competition for Corporate Charters and the Lesson of Takeover Statutes*, 61 FORDHAM L. REV. 843 (1993) (discussing competition among states for the business of corporate charters).

[231] *See supra* note 153 and accompanying text.

Technology's Information Security Committee is attempting to address these problems with its Digital Signature Guidelines. At this writing, the first, still unofficial, exposure draft is being revised.[232] This Article has avoided discussing the Draft Guidelines because of their preliminary nature and the likelihood that they might change significantly by the time this Article is published. Whatever their final form, however, it is already clear that the Guidelines stand a chance of influencing both the practice and regulation of CAs and that they warrant careful reading.[233]

CONCLUSION

Persons who are not previously acquainted, but wish to transact with one another via computer networks such as the Internet, will need a means of identifying or authenticating each other. One means of achieving this is to introduce a trusted third party into the bilateral relationship. This third party, a Certification Authority, can vouch for a party by issuing a certificate identifying her, or attesting that she possesses a necessary qualification or attribute. CAs may become essential to much, but not all, electronic commerce. Although at this writing there are few CAs in operation, and what electronic commerce takes place rarely relies on certificates, the dollar value of electronic commerce is forecast to grow quickly. If it does, the demand for CA's services should grow rapidly as well.

Outside the states of Utah and Washington, which have passed comprehensive digital signature acts but currently have no CAs qualified to take advantage of their terms, state rules likely to be applicable to CAs are unclear. Basic concepts, such as whether a CA's sale of a certificate is the sale of a "good," a "service," or the mixture of the two for UCC Article 2 purposes, remain to be determined. State common-law rules concerning the liability of a CA for negligent misrepresentations in a certificate are anything but uniform, and in some cases likely to be unclear also.

The more general lack of regulatory and legal standardization that these examples evince may prove to be a large impediment

---

232 ABA Draft Guidelines, *supra* note 4. The comment period ended January 15, 1996.

233 In the spirit of full disclosure, I should confess that I am a quondam member of the ABA's Information Security Committee and was involved in drafting parts of the draft Guidelines.

to the development of reliable electronic commerce. A national—or even possibly international—standard for accurately signaling what a certificate promises, and the extent to which a certificate can reasonably engender reliance, may be needed. Such a standard is unlikely to emerge until the relevant legal rules that already exist are identified; the development of standards is also likely to be retarded by the great diversity of legal regimes in different jurisdictions that may be involved in a single transaction. Whether it would be best to produce the needed legal standardization through legislation, the judicial process, or market mechanisms such as the bargaining process and the usages of trade, is debatable. However, until some standardization is achieved, users of digital signatures will find it difficult to determine what degree of commercial reliance to place on a representation in a certificate.

Standards aside, the current uncertainty about the law creates a climate in which CAs have an enormous incentive to understate the reliability of their certificates in order to avoid exposure to liability whose contours are difficult to predict. This understandable behavior undermines the justified reliance that CAs should be designed to achieve; if it persists, legislation to balance CA incentives and liability is likely to become necessary. State legislation holds out the promise of clearer rules and the avoidance of much litigation, but today this clarity comes at the price of having to determine the distributional consequences of mistakes by CAs and the people who use certificates before there is any significant evidence of the nature and patterns of certificate use and abuse.

After a reasonable period of experimentation in which market-driven certificates that do not purport to be worthless have a chance to surface, it will be appropriate to consider whether the national interest in a functioning national information infrastructure might be better served by uniform national rules. The CA equivalent of Delaware's corporate law might emerge from a competition among state regulatory authorities. If not, uniformity could be achieved via the traditional channels for state law harmonization, such as model laws and uniform acts, or by federal legislation. In addition to these national standards, at least minimal international norms for certificate recognition and CA regulation will become increasingly necessary as electronic commerce becomes more global.