UIC John Marshall Journal of Information Technology & Privacy Law

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

Article 9

Spring 1999

The Liability of Certification Authorities to Relying Third Parties, 17 J. Marshall J. Computer & Info. L. 961 (1999)

Michael J. Osty

Michael Pulcanio

Recommended Citation

Michael J. Osty & Michael J. Pulcanio, The Liability of Certification Authorities to Relying Third Parties, 17 J. Marshall J. Computer & Info. L. 961 (1999)

THE LIABILITY OF CERTIFICATION AUTHORITIES TO RELYING THIRD PARTIES

by MICHAEL J. OSTY†
& MICHAEL J. PULCANIO††

I. INTRODUCTION

As Internet technology continues to expand and individuals continue to "log-on" at an ever-increasing rate, business transactions via computers have quickly expanded. Electronic commerce has become a widely accepted way of entering transactions and consummating deals. Consequently, millions and even billions of dollars change hands in transactions utilizing electronic commerce daily. These transactions are conducted between individuals who often have had no prior business relationship with each other. As a result, the need for a trusted third party to authenticate these transactions has become absolutely necessary. However, the laws governing the financial responsibility of these trusted third parties, or certification authorities, have not been thoroughly developed.

The need for digital certification authorities evolved due to the growth of computer and Internet technology. Unfortunately, legislation and strict guidelines for monitoring the performance of certification authorities has not evolved as rapidly. A few states have drafted legislation to address the activities of certification authorities, while others have only just begun the process. A number of states have pending legislation concerning digital signatures.[1] Despite the recent legislative ac-

† B.A., Purdue University; J.D., The John Marshall Law School. Mr. Osty is an attorney with the Chicago law firm of Lowis & Gellen.

†† B.A., Northern Illinois University; J.D., The John Marshall Law School. Mr. Pulcanio is an attorney with the Chicago law firm of Clausen Miller.

[1] *See* Anthony Martin Singer, *Electronic Commerce: Digital Signatures and the Role of the Kansas Digital Signature Act*, 37 WASHBURN L.J. 725, 731 n.50 (1998). For a comprehensive review of digital signature legislation, see the McBride, Baker & Coles Web page regarding the summary of electronic commerce and digital signature legislation, at <http://www.mbc.com/ds_sum.html> (last visited on April 9, 1999). As of this writing, forty-nine states have enacted or are considering some form of digital signature legislation. Massachussetts is the only state that has not yet introduced any legislation. *Id.*

tivity, one very important area which continues to lack thorough and uniform coverage by current statutory schemes, is the financial responsibility of certification authorities. Ultimately, all state legislation must address the financial responsibility of certification authorities, because the transactions that they authenticate will undoubtedly have great financial importance to the parties involved.

This article focuses on the current liability standards and responsibilities of the trusted third parties known as certification authorities. Part II explains the certification process and the role of the certification authority. Part III identifies the current liability standards of certification authorities to relying third parties.

II. DIGITAL SIGNATURES AND THE PROCESS OF CERTIFICATION

Digital signature legislation is designed to promote the same type of transactions that were traditionally memorialized with written signatures. Only recently have parties utilized digital signatures to complete their electronic transactions. The need for such technology can certainly be attributed to the evolution and increased usage of computers for Internet commerce.

In theory the process is very simple. Individuals, businesses, corporations and other like entities can conduct their business via open systems, such as the Internet. Instead of bringing signed documents to a notary public, an individual, known as a "subscriber," can apply for a certificate and use the certificate as a form of identification for conducting electronic transactions. The receiving party, known as the "recipient," has the option of entering into the transaction based on the level of security or trust that he places in the certificate. The Certification Authority ("CA"), is the unbiased, trusted third party, who confirms, via the issued certificate, the subscriber's identity and his or her relationship to the digital signature.

The actual process that a CA undertakes to authorize a signature is referred to as "asymmetric encryption technology."[2] Encryption is a mathematical system that scrambles the data in electronic messages

[2] *See generally Digital Signatures Guidelines*, 1996 A.B.A. SEC. OF INFO. SECURITY COMMITTEE OF SCI. TECH. (1996) (hereinafter *Digital Signatures Guidelines*) (*also available at* <http://www.abanet.org/scitech/ec/isc/dsgfree.html>) (visited on Feb. 24, 1999). The ABA defines asymmetric cryptosystem as: "[a] system which generates and employs a secure key pair, consisting of a private key for creating a digital signature, and a public key to verify a digital signature." *Id.* at § 1.3. Asymmetric cryptography is the technical foundation for digital signatures. *Id.* at § 1.3.1. "The asymmetric cryptosystem used for creating and verifying digital signatures may include functions for encrypting or decrypting the message, in which case the private key of the key pair is used for encryption and the public key is used for decryption." *Id.* at § 1.3.3.

making them unreadable to individuals not possessing the proper information to decode the message.[3] The following sections describe the process of encryption and how it is used to create and verify a digital signature.

A. Private Keys and Public Keys

A digital signature is the computerized version of a written signature.[4] However, as simple as that may sound, the process is much more complex. Utilizing cryptography, digital signatures are attached to electronic documents employing electronic "keys."[5] The "keys" consist of "private keys" and "public keys."[6] The "private keys" create the digital signature.[7] "Private keys" are created by the document's signer and are known only by him.[8] To verify the signature, a relying party utilizes the widely known "public key."[9]

If the process is designed and implemented properly, it is almost impossible to discover the private key from known information of the public key.[10] Therefore, even though many people are aware of the public key of a particular signer and use it to verify his signature, they are unable to discover his private key and use it to forge his digital signature.[11]

B. The Digital Signature

The digital signature is created in several steps. The signature is made up of a series of digits representing a combination of the document and the unique computer-generated code, known as a "hash."[12] The signer first uses a "hash function" to encrypt the "message" that the

[3] *See* Singer, *supra* note 1, at 728, *citing* Gary W. Fresen, *What Lawyers Should Know About Digital Signatures*, 85 Ill. B.J. 170, 171 (1997).

[4] *See* Michael L. Closen & Jason Richards, *Notaries Public-Lost in Cyberspace, or Key Business Professionals of the Future?*, 15 J. Marshall J. Computer & Info. L. 703, 735 (1997).

[5] *See* Closen & Richards, *supra* note 4, at 735; *see also* Information Security Committee, Section of Science and Technology, American Bar Association, Tutorial, 38 Jurimetrics J. 243, 248 (1998) (hereinafter Security Committee). Cryptography is a segment of applied mathematics that focuses on transforming messages into unintelligible forms and back again. *Id.*

[6] *Id.* at 248.

[7] *See Digital Signature Guidelines*, *supra* note 2, at § 1.24.

[8] *See* Closen & Richards, *supra* note 4, at 735.

[9] *See Digital Signature Guidelines*, *supra* note 2, at § 1.25. In the event that various individuals need to verify the signer's digital signature, the public key must be made known to all of them. *See* Security Committee, *supra* note 5, at 248. Usually, the public key can be made known to others through publication in an on-line repository where it is readily accessible. *Id.*

[10] Security Committee, *supra* note 5, at 248-249.

[11] *Id.* at 249.

[12] *Id.*

signer is going to sign. The "hash function" is a computer program used to create a unique hash result.[13] These digits are a combination of letters, numbers, and/or symbols.[14]

Once the hash result is created, the message's signer types in a pseudo-PIN number, and then the private key generates a long string of numbers and letters which represents the signature.[15] The computer-generated signature, like the hash result, is unique to each message.[16]

To verify the signature of a digitally signed message, the recipient reverses the process.[17] Through the use of a software program on the recipient's computer, the message recipient computes a new hash result using the same hash function that created the digital signature.[18] With the public key of the signer and new hash result, the recipient then must determine two components to verify the signature.[19] First, whether the digital signature was created with the private key matching the public key;[20] and second, whether the new hash result matches the original hash result created at the time the message was signed.[21] A digital signature is "verified" if the public key successfully verifies the private key of the signer and the hash results match.[22] This indicates that the document has not been altered between the sender and receiver.[23]

C. The Role of the Certification Authority in the Certification Process: Trusted Third Party

This article focuses on the responsibilities and liabilities of the trusted third party in the digital signature authentication process. This party is known as a certification authority or "CA."[24] A CA is an independent third party who ties a particular person to his public key.[25] The CA plays a vital role in creating an environment of trust in which

[13] *Id.* at 250.

[14] *Id.* at 248-49.

[15] Security Committee, *supra* note 5, at 248-49.

[16] *Id.* at 249 (stating that "any alterations to a message produces a new hash result when the same hash function is used").

[17] *Id.*

[18] *Id.* at 249-50.

[19] *Id.* at 250-51.

[20] Security Committee, *supra* note 5, at 250-51.

[21] *Id.*

[22] *Id.*

[23] *Id.* at 251.

[24] *See* Charles R. Merrill, *The Accreditation Guidelines — A Progress Report on a Work in Process of the ABA Information Security Committee*, 38 JURIMETRICS J. 345, 349 (1998).

[25] *See* Closen & Richards, *supra* note 4, at 703. Certification authorities are also commonly referred to as cybernotaries. *Id.*; *see also* Security Committee, *supra* note 5, at 253.

parties can conduct confidential and trustworthy communications.[26] These elements are essential to the successful operation of a public key infrastructure.[27]

1. *Public Key Infrastructure*

The foundation of the environment where parties use public and private keys is known as a "public key infrastructure" or PKI.[28] A PKI is a group of people providing necessary services to allow public key technology users to establish the authenticity of the public keys of the people with whom they are transacting business.[29] PKIs require the use of one or more CAs that serve the function of binding a particular person to a specific public key.[30]

CAs play an important role in PKIs because the CA establishes a trustworthy environment for digital signatures to exist in electronic commerce.[31] Strangers entering into transactions with other strangers in the PKI rely on the CA to verify identities and signatures.[32] Without the CA, a party would be unable to verify quickly and accurately whether the tendered public key was in fact that of the document signer.[33] In issuing a certificate, the CA provides assurance that the communications between the strangers is confidential and authentic.[34]

2. *The Process of Issuing a Certificate*

The process by which a CA creates and issues a certificate can be described in several steps. First, the CA offering its certification services creates its own public and private key pair in the public key cryptography system.[35] The CA's public key is widely available and recipients of messages trust the CA to have adequately protected its private key from becoming available to others.[36]

[26] Security Committee, *supra* note 5, at 254; *see also* Timothy Tomlinson, *Contracts Over the Internet Pave the Way for a Host of New Woes*, 14.2 COMPUTER L. STRATEGIST 1 (1997). A digital certificate is a digital document that the holder of the private key receives from the certification authority trusted by the holder of the private key and the recipient of a message signed with that private key. *Id.* The sender's attachment of a digital certificate to its signature eliminates the problem of identifying the holder of the private key and attaching its private key to a contract. *Id.*

[27] Security Committee, *supra* note 5, at 254.

[28] *Id.* at 253.

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] Security Committee, *supra* note 5, at 253.

[33] *Id.* at 253-54.

[34] *Id.* at 254.

[35] *See* Tomlinson, *supra* note 26, at 3.

[36] *Id.*

An applicant wishing to digitally sign a document creates a public and private key pair and then applies to the CA for a certificate.[37] The certificate is the electronic record that will match the applicant to his public key and lists the public key as the "subject" of the certificate.[38] The CA then takes the record containing the information to identify the applicant, who now is considered a "subscriber," the subscriber's public key, and the information identifying the CA, and encrypts the record by signing it using its private key.[39]

The information collected and verified by the CA, as well as the CA's signature, serve as the completed certificate. The certificate is then made publicly available in a "repository" maintained by the CA or someone else. When the recipient receives the digitally signed message of the subscriber, which references the certificate, the recipient can choose to rely on the certificate and thereby become a "relying party." The recipient then goes to the repository, accesses the certificate that confirms the association of the signer to his public key, and retrieves a copy of the public key to decrypt the digital signature. Successfully decrypting the message with the public key is "extraordinarily reliable evidence" that the message received was sent by the person holding the corresponding private key.[40]

3. *Verifying Certification Authorities Signatures*

Verifying the issuing CA's digital signature on the certificate is accomplished "by using the public key belonging to the CA listed in another certificate by another CA, and that other certificate can then be authenticated by the public key listed in yet another certificate."[41] The person

[37] *Id.*

[38] *See* Security Committee, *supra* note 5, at 254.

[39] *See* Tomlinson, *supra* note 26, at 3-4.

[40] R.R. Jueneman & R.J. Robertson Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 JURIMETRICS J. 427, 439 (1998).

[41] *See Digital Signature Guidelines*, *supra* note 2, at 18. Various models exist which implement different strategies for the certification of the public keys of certification authorities who issue certificates. *See* Security Committee, *supra* note 5, at 255. A person can continue to verify the validity of each certification authority until the person is convinced that the signature is genuine. *Id.*
Specific examples include:

> (i) a multi-level hierarchical structure back to a single "root," where public keys of issuing authorities are certified by the next higher-level certification authority; (ii) a flatter hierarchical structure where a single "root" might directly certify the public keys of all issuing authorities below it; (iii) a single level of issuing authorities which "cross-certify" each others' public keys; or (iv) a "system in which each issuing authority's public key is certified in some reliable manner without reference to a second certification authority.

Digital Signature Guidelines, *supra* note 2, at 18 n.34. By definition, the "public key of the 'root' certification authority" in a hierarchical system is self-authenticating. *Id.*

relying on the digital signature can continue to verify each certificate until he reaches a CA that the person recognizes or trusts.[42] In each instance, the issuing CA is required to digitally sign its own certificate during the operational period of the other certificate used to verify the CA's digital signature.[43] In Illinois, the "operational period of a certificate" begins when the certificate is issued by a CA and ends on the date and time the certificate is designated to expire.[44]

D. Unreliable or Fraudulent Certificates

While successfully decrypting a message provides assurance that the sending party holds the private key and the message has not been altered, such electronic transactions are still susceptible to fraud. A party may attempt to obtain the private key of a CA through theft. Once obtained, the party could issue certificates at will. Another method might be to attempt a cryptanalytic attack on the CA's key pair and thereby discover the method for creating the key.

Even if a CA changes keys often, a party in possession of an old key pair could forge an older certificate attesting to a bogus public key. The party could then create a fraudulent document and authenticate it with the back dated certificate. Obtaining the private key of a CA is not the only method of committing digital signature fraud.

A subscriber can create an unreliable or fraudulent certificate by misrepresenting his true identity to a CA.[45] If the party successfully certifies a key pair in someone else's name, the scenarios for loss are almost limitless. One possible scenario might be where John steals Mark's identification and checkbook. John then generates a key pair and has the public key certified by a CA in Mark's name. Once John obtains the certificate, he could possibly sign Mark's name electronically to request to withdraw thousands of dollars from Mark's known bank account.

The human element of issuing a certificate is also susceptible to corruption. A party, say John, might bribe an employee of a CA responsible for issuing certificates. If this corrupt employee retains sole responsibility for final issuance, John could easily get a public key certified in anyone's name. A recipient of such a certificate would be unable to tell that it was bogus because the certificate would contain a complete and verifiable certificate chain.[46]

[42] *Id.* at 18.

[43] *Id.*

[44] *See* Illinois Electronic Commerce Security Act, H.B. 3180, 90th Leg., 1997 Reg. Sess. (Ill. 1997).

[45] *See Digital Signature Guidelines*, *supra* note 2, at 19-20.

[46] Sample scenarios taken from RSA Laboratories' website at <http://www.rsa.com/rsalabs/faq/html/4-1-3-14.html> (visited on Feb. 24, 1999).

Also, a certificate may have been reliable and valid when issued, and only later become unreliable.[47] It may be that a business subscriber lost control of its private key. A disgruntled employee may have stolen the key and thereafter, entered into transactions benefiting him for hundreds or thousands of dollars.

In each of the scenarios above, the recipient of the digital signature was unaware that the signer was an imposter. The recipient may have transacted business with the impersonated signer before, and therefore, had no reason to distrust the public key. Or, the recipient may have checked the certificate chain and found that each certificate was verifiable and therefore chose to rely on any one of the certificates. In each case, the recipient has suffered a loss based on his reliance on the bogus certificate.

Having suffered a loss, the relying party now seeks redress from the imposter. Assuming the imposter can be located, he is likely unable to repay the losses caused. Therefore, the relying party turns to the CA that issued the fraudulent certificate for redress. The following section discusses the liability standards of CAs to third parties who rely on issued certificates.

III. LIABILITY STANDARDS AND RESPONSIBILITES OF CERTIFICATION AUTHORITIES TO RELYING PARTIES

In the scenarios above, the recipient had the option of choosing to rely or not rely on a particular certificate. The recipient may choose to rely on one or several certificates attached in a hierarchy on a signed document. Once he chooses to rely, and even before reliance, the CA must conform to certain standards in issuing the certificate. What these standards are, and the resulting liability of a CA for violating these standards, depends upon state statute and/or the contract language and common law governing the agreement between the CA and relying party.

A. Statutory Liability Standards Of Certification Authorities

Currently, 49 states have enacted legislation governing the use of electronic or digital signatures.[48] Several state statutes only authorize the use of electronic signatures for transactions with government entities.[49] Despite the ever increasing growth of electronic commerce and the concurrent rise in the potential for fraud or financial loss, only four of these states have enacted comprehensive legislation addressing the lia-

[47] *See* Security Committee, *supra* note 5, at 255-56.

[48] *See* McBride, *supra* note 1, at 726 n.50-52.

[49] *See, i.e.*, Alabama, Arizona, California, Delaware, Idaho, Indiana, Maryland, Minnesota, Missouri, Nebraska, Nevada, New Mexico, Rhode Island and Texas.

bility standards of CAs to relying parties in public and private communications.

Utah enacted the seminal digital signature statute in 1995.[50] This statute led the way in delineating the standards of conduct and liability of a CA in issuing a certificate for use in public and private communications. Following Utah's lead, and mirroring Utah's statute in many respects, Washington,[51] Minnesota[52] and Illinois[53] addressed the issue of CA liability to a relying party. The following section highlights those portions of the statutes that cover the liability of a CA to a party relying on an issued certificate.

1. *Utah Digital Signature Act*

First to authorize commercial use of digital signatures, the Utah Digital Signature Act ("Utah Act") established the qualification standards and licensing requirements of CAs.[54] In addition, it established the minimum standards of practice of CAs in a public key infrastructure (PKI).[55] Importantly, it established the warranties and obligations of a CA upon issuance of a certificate,[56] the recommended reliance limits and liability of a CA on a certificate,[57] as well as the means and method of recovery against a CA for injuries caused by reliance on a defective certificate.[58]

Under the Utah Act, a CA must use a "trustworthy system" to perform its services.[59] According to § 46-3-303 of the Act, by issuing a certificate, a licensed CA certifies to all who reasonably rely on the information contained in the certificate that:

> (a) the information in the certificate and listed as confirmed by the certification authority is accurate;
> (b) all foreseeable information material to the reliability of the certificate is stated or incorporated by reference within the certificate;
> (c) the subscriber has accepted the certificate; and
> (d) the licensed certification authority has complied with all applicable laws of this state governing issuance of the certificate.[60]

[50] *See* UTAH CODE ANN. §§ 46-3-101 to -504 (West Supp. 1997).

[51] *See* WASH. REV. CODE ANN. §§ 19.34.010 to .903 (West Supp. 1998).

[52] *See* MINN. STAT. ANN. § 325K. (West Supp. 1998).

[53] *See* Illinois Electronic Commerce Security Act, H.B. 3180, 90th Leg., 1997 Reg. Sess. (Ill. 1997).

[54] UTAH CODE ANN. § 46-3-201.

[55] *Id.* at § 46-3-301.

[56] *Id.* at § 46-3-303.

[57] *Id.* at § 46-3-309.

[58] *Id.* at § 46-3-310.

[59] UTAH CODE ANN. § 46-3-301(1).

[60] *Id.* at § 46-3-303(3).

Should the CA breach a warranty resulting in damage to a relying party, there are limitations to the amount of recovery. The Utah statute recommends both reliance and liability limits to a certificate. With regard to reliance limits, the Utah Act, § 46-3-309, provides:

> (1) By specifying a recommended reliance limit in a certificate, the issuing certification authority and the accepting subscriber recommend that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit.[61]

In addition to the provisions of the Utah Act, the CA itself can establish limitations on its liability through its own operating procedures. The Act further provides that unless a CA waives the limitations of the Act in its operating procedures, the CA is not liable in excess of its recommended reliance limits for "any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature . . ." the CA complied with the material requirements of the Act.[62] Such material requirements consist of using only a "trustworthy system" to perform its services and not conducting its business in a manner which causes unreasonable risk of loss.[63]

However, according to the Utah Act, even if the loss is caused by reliance on a misrepresentation the CA is required to confirm, the CA's liability is still limited to no more than the recommended reliance limit on the certificate. This effectively limits recoverable damages to only direct and compensatory damages and excludes punitive damages, damages for lost profits and/or damages for pain and suffering.[64]

The Utah Act provides a built-in method of recovery to aid injured relying parties. The Act requires that, to obtain a license, a CA must file a "suitable guaranty"[65] with the Division of Corporations and Commercial Code ("Division") within the Utah Department of Commerce.[66] This guaranty ensures that a certain sum of money is available for recovery. In order to recover against this guaranty, an injured party or claimant must file a written notice with the Division within two years after the occurrence of the violation.[67] The written notice must provide the amount and grounds of the claim as well as any other pertinent information required by rule of the Division.[68] The Act also provides for recovery of attorneys' fees and court costs.[69]

[61] *Id.* at § 46-3-309.

[62] *Id.* at § 46-3-303.

[63] *Id.*

[64] UTAH CODE ANN. § 46-3-204.

[65] *Id.* at § 46-3-103(34)(a).

[66] *Id.* at § 46-3-201(1)(d).

[67] *Id.* at § 46-3-310(4)(b.

[68] *Id.* at § 46-3-310(3).

[69] UTAH CODE ANN. § 46-3-310(2).

Recovery against a guaranty is intended to be faster and easier than filing a civil suit. However, the available recovery against the guaranty may be limited. As previously stated, the claimant can only recover an amount that does not exceed the recommended reliance limit on the certificate. More importantly, the total liability of the guaranty cannot exceed the maximum dollar amount of the guaranty.[70] Therefore, if prior claims have been made against the guaranty during its effective term, the amount available to additional claimants will be diminished accordingly.

2. *Washington Digital Signature Legislation*

The state of Washington modeled its Washington Electronic Authentication Act ("Washington Act") after the Utah Act. The Washington Act was enacted on March 29, 1996. Like the Utah Act, the Washington Act contains provisions that detail the warranties and obligations of a CA to a relying party. The Washington Act also recommends reliance limits on certificates and limits the kind of reliance damages recoverable.[71]

The warranties and obligations of a CA to a relying party are practically identical to those of the Utah Act.[72] In addition, a CA must use a "trustworthy" system[73] to conduct its operations as well as provide a "suitable guaranty,"[74] made payable to the Secretary of State, for the benefit of claimants.[75]

Also, like the Utah Act, the Washington Act recommends that a recipient not rely on a certificate to the extent that the risk of loss is greater than the certificate's reliance limit.[76] Relying parties should be aware that a CA is protected completely from liability on a false or forged digital signature, provided that it complied with the material requirements of Chapter 19.34 of the statute.[77] As to liability for losses caused by reliance on a misrepresentation the CA was required to confirm, those losses are limited to direct damages only, unless the CA otherwise

[70] *Id.*

[71] *Id.* at § 19.34.280.

[72] *Id.*

[73] WASH. REV. CODE ANN. § 19.34.100(e) (West 1998). The Washington Act defines a trustworthy system as "computer hardware and software which: (a) are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; and (c) are reasonably suited to performing their intended functions." *Id.*

[74] *Id.* at § 19.34.020(35). Under section 19.34.030(b), the Act provides that when determining the amount of the guaranty, the Secretary is to consider the amount of burden the suitable guaranty places on the CA as well as the "assurances of quality and financial responsibility it provides to persons who rely on certificates issued by licensed certification authorities." *Id.*

[75] *Id.*

[76] *Id.* at § 19.34.280.

[77] WASH. REV. CODE ANN. §§ 19.34.010 to .903 (West Supp. 1998).

waives the statutory limitations.[78]

While the CA may be able to limit the amount of its liability for certain losses, it is not relieved of its liability for breach of any of the warranties or certifications given upon issuance of a certificate.[79] Moreover, the CA cannot disclaim the warranty and obligation of good faith, but it can modify by agreement or notice, the standard by which good faith is measured so long as the standard is not manifestly unreasonable.[80]

3. *Minnesota Digital Signature Legislation*

The Minnesota Electronic Authentication Act ("Minnesota Act") was enacted on May 19, 1997.[81] Modeled after the Utah Act, Minnesota's Act recommends reliance limits on certificates and sets forth the warranties and obligations to parties who rely on an issued certificate.[82] As part of its licensure conditions, the Minnesota Act requires the CA to use a "trustworthy system"[83] and file a "suitable guaranty," as well as main-

[78] *Id.* at § 19.34.280.

[79] *Id.* at § 19.34.280(3).

[80] *Id.*

[81] MINN. STAT. ANN. § 325K.05 Subd. 1 (West Supp. 1998). To obtain or retain a license, a certification authority must:

> (1) be the subscriber of a certificate published in a recognized repository;
> (2) employ as operative personnel only persons who have not been convicted within the past 15 years of a felony or a crime involving fraud, false statement, or deception;
> (3) employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of this chapter;
> (4) file with the secretary a suitable guaranty, unless the certification authority is a department, office, or official of a federal, state, city, or county governmental entity, that: is self-insured;
> (5) use a trustworthy system, including a secure means for limiting access to its private key;
> (6) present proof to the secretary of having working capital reasonably sufficient, according to rules adopted by the secretary, to enable the applicant to conduct business as a certification authority;
> (7) register its business organization with the secretary, unless the applicant is a governmental entity or is otherwise prohibited from registering; and
> (8) comply with all further licensing requirements established by rule by the secretary.

Id.

[82] MINN. STAT. ANN. § 325K.05 Subd. 3 (West Supp. 1998). Warranties to those who reasonably rely. By issuing a certificate, a licensed certification authority certifies to all who reasonably rely on the information contained in the certificate that:

> (1) the information in the certificate and listed as confirmed by the certification authority is accurate;
> (2) all information foreseeability material to the reliability of the certificate is stated or incorporated by reference within the certificate;
> (3) the subscriber has accepted the certificate; and
> (4) the licensed certification authority has complied with all applicable laws of this state governing issuance of the certificate.

[83] *Id.* at Subd. 1.

tain sufficient working capital to conduct its business.[84]

4. *Illinois Digital Signature Legislation*

Known as the "Electronic Commerce Security Act" ("Illinois Act"), the Illinois Act takes effect July 1, 1999.[85] However, the Illinois Act does not mirror the form and liability standards of the Utah Act and its progeny. For example, the requirement that the CA perform its services in a "trustworthy manner," is not absolute. The Illinois Act requires that a CA maintain its operations and perform its services in a trustworthy manner, except as conspicuously set forth in its certificate practice statement ("CPS"). This allows the CA to modify its operations standard and conduct its services in a different manner than that defined in the statute.[86]

The Illinois Act does not specifically address the manner of recourse against a CA nor recommend reliance limits on certificates. However, where a CA has no relevant governing standards or procedures in its CPS, an injured relying party can utilize the standards of liability and obligations set forth in the statute as a measure of proper performance. The Illinois Act, Section 15-315, contains the following language regarding the CA's representations to relying third parties upon issuance of a certificate:

> (a) By issuing a certificate with the intention that it will be relied upon by third parties to verify digital signatures created by the subscriber, a certification authority represents . . . to any person who reasonably relies on information contained in the certificate, in good faith and during its operational period, that:
>
>> (1) the certification authority has processed, approved, and issued, and will manage and revoke if necessary, the certificate in accordance with its applicable certification practice statement stated or incorporated by reference in the certificate or of which such person has notice, or in lieu thereof, in accordance with this Act or the law of the jurisdiction governing issuance of the certificate;
>>
>> (2) the certification authority has verified the identity of the subscriber to the extent stated in the certificate or its applicable certification practice statement, or in lieu thereof, that the certification authority has verified the identity of the subscriber in a trustworthy manner;
>>
>> (3) the certification authority has verified that the person requesting the certificate holds the private key corresponding to the public key listed in the certificate; and

[84] *Id.* The CA must file a suitable guaranty unless it is a department, office, or official of a federal, state, city or county governmental entity that is self insured. *Id.* at (4).

[85] 5 ILL. COMP. STAT. 175/1-101 et seq. (effective July 1, 1999).

[86] 5 ILL. COMP. STAT. 175/5-105.

> (4) except as conspicuously set forth in the certificate or its applicable certification practice statement, to the certification authority's knowledge as of the date the certificate was issued, all other information in the certificate is accurate, and not materially misleading.[87]

5. *Other CA Liability Legislation*

The majority of state statutes have yet to address the issue of CA liability to relying parties in public and private communication. However, several states have recognized the need for legislation in this area or have enacted civil or criminal penalties for violation of their electronic commerce act.[88] While not addressing liability standards directly, Mississippi, in recognition of the potential for loss to third parties, requires both adequate capitalization of private CAs and that the CA maintain a registered agent in the state.[89]

The currently enacted legislation protecting relying parties is neither uniform nor widely available. Consequently, the majority of digital signature transactions and concurrently issued certificates will not be covered by state statute. Instead, the standards of liability and obligations of a CA when issuing a certificate will be defined by the CA itself.

B. Contractual Liability Standards Of Certification Authorities

The recipient of a certified digital signature can choose whether or not to rely on the signature based on the perceived trustworthiness of the attached certificate. If the recipient chooses to rely on the certificate, both statute and contract may govern the terms of that reliance. However, digital signature statutes that govern the liability standards of certification authorities are neither widely available nor uniform throughout the United States. As a result, contract clauses will most often dictate the terms of the recipient's reliance.

CAs, through their own documentation, have endeavored to define their standard of liability and responsibilities to relying parties. Each CA develops its own contractual language, and thereby defines the relationship, responsibilities and obligations among the parties to the certificate. Through the use of well-drafted documents, CAs can make broad or narrow disclaimers, warnings, disclosures, and limitations on their

[87] 5 Ill. Comp. Stat. 175/15-315.

[88] CA Gov't Code § 16.5 (West Supp. 1998); *Electronic Commerce Act*, 1998 N.C. Sess. Laws 127; *The Electronic Signature Act*, Or. Rev. Stat. § 192.825 et. seq. (1997) (stating that the Director of the Dept. of Business Services shall have the authority to revoke or suspend certificates or registrations issued by the Director). *Id.*

[89] Miss. Code Ann. § 25-63-7 (1997).

liability.[90]

The basic documents that define the standards, practices, and responsibilities of the CA are the Certificate Practice Statement ("CPS") and the Relying Party Agreement ("RPA"). These documents, subject to applicable law, determine the liability standards of the CA and the availability of recovery by an injured recipient. These documents form the basis of a contractual relationship between the CA and relying party(s). The following sections discuss the basic elements of these two contracts.

1. *Certificate Practice Statement (CPS)*

The CPS is defined by the "Digital Signature Guidelines" as "[a] statement of the practices that a CA employs in issuing certificates."[91] A CPS describes in detail how a CA issues and manages certificates and maintains the PKI. The CPS also controls the certification process and its use. It is intended to legally bind the participants in the digital signature process as well as the users of the PKI. [92]

The CPS also details the standards and obligations that a CA employs when issuing a certificate. This includes warranting and/or promising to perform certain obligations and provide specific services. The following sample warranty provision was taken from a CA known as VeriSign:

> Issuing authorities (and VeriSign, to the extent specified in the referenced CPS sections) warrant and promise to:
>
> • provide the infrastructure and certification services, including the establishment and operation of the VeriSign repository, as delineated in [the CPS],
>
> • provide the controls and foundation for VeriSign's PKI, including IA key generation, key protection, and secret sharing procedures, presented in [the CPS],
>
> • perform the application validation procedures for the indicated class of certificate as set forth in [the CPS section],
>
> • issue certificates in accordance with CPS [applicable section #] and honor the various representations to subscribers and to relying parties presented in [the CPS section #],
>
> • publish accepted certificates in accordance with CPS [applicable section #],

[90] Stephen S. Wu, *Incorporation By Reference And Public Key Infrastructures: Moving The Law Beyond The Paper-Based World*, 38 JURIMETRICS J. 317, 326 (1998).

[91] *Digital Signature Guidelines*, *supra* note 2, at § 1.8.

[92] *See* Veronique Wattiez Larose, *Brief Essay on the Notion of and Rules Relating to Incorporation by Reference in Civil Law Systems*, 38 JURIMETRICS J. 295 (1998). The comprehensive provisions of a CPS describing practices, rights and obligations, are lengthy and for practical purposes, cannot be placed directly on each issued certificate. *Id.* Therefore, the CA incorporates the CPS by reference in the issued certificate. *Id.* Through incorporation by reference, the CPS intends to legally bind parties utilizing the CA's services. *Id.*

> - perform the obligations of an IA and support the rights of the subscribers and relying parties who use certificates in accordance with CPS [section #],
> - suspend and revoke certificates as required by CPS [section #],
> - provide for the expiration, re-enrollment, and renewal of certificates as stated in CPS [section #], and
> - comply with the provisions contained in CPS [section #]. . .

Additionally, IAs (Issuing Authorities) and VeriSign warrant that their own private keys are not compromised unless they provide notice to the contrary via the VeriSign repository, for example:

> ISSUING AUTHORITIES AND VERISIGN MAKE NO OTHER WARRANTIES AND HAVE NO FURTHER OBLIGATIONS UNDER THIS CPS.

Having set forth the service warranties and promises, the CPS contains provisions disclaiming and limiting any additional warranties or obligations. The following disclaimer language is taken from VeriSign's CPS:

> EXCEPT AS EXPRESSLY PROVIDED IN THE FOREGOING [CPS section #], ISSUING AUTHORITIES AND VERISIGN DISCLAIM ALL WARRANTIES AND OBLIGATIONS OF ANY TYPE, INCLUDING ANY WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF INFORMATION PROVIDED, AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE AND LACK OF REASONABLE CARE.

In the event a CA breaches a warranty, which it has not effectively disclaimed, the CPS can and will contain language and mechanisms by which the CA can limit its financial liability. In order to avoid the specter of unlimited liability, a CA can issue certain "classes" of certificates with applicable liability caps. The following table provides an example of such a structure:

	Liability Caps
Class 1	$ 100.00 US
Class 2	$ 5,000.00 US
Class 3	$100,000.00 US

The class of certificate the relying party received limits the CA's liability on that certificate. The CA adds additional language to state that the aggregate liability of a CA to all persons claiming loss due to reliance on a specific certificate is limited to the liability cap of the certificate class. Unless otherwise stated, this aggregate liability includes claims for damages of all types. Through the CPS, the CA will exclude liability for other damages such as special, incidental, indirect or lost profits.

Through careful drafting of the CPS the CA can set forth the standards of practice and limit its potential, liability when issuing a certificate. Inserting this language by reference into a certificate, the CA creates an enforceable agreement among the parties to the certificate.[93] If a recipient chooses to rely on the certificate, thereby utilizing the certification services of the CA, the recipient binds him or herself to the terms of the CPS.

However, the CPS is not the only document that sets forth the liability standards and limitations of the CA to a relying party. The actions of a recipient when s/he relies on a certificate or even investigates the validity of a certificate may bind him to the terms of an additional contract, known as the "Relying Party Agreement."

2. *Relying Party Agreement (RPA)*

By using the information or services provided by the CA, a relying party may subject himself to the terms of a Relying Party Agreement ("RPA"). Like the CPS, the RPA notifies the relying party of the warranties, disclaimers, classes of certificates, liability limits and limitations of damages applying to an issued certificate. An RPA can be drafted so that a relying party makes certain acknowledgements regarding the certificate and its use by the relying party.

Once a recipient takes an action sufficient to make him or herself a "relying party," he is bound by the terms of the RPA. The RPA typically applies and restates the same warranty provisions, liability limitations and caps detailed in the controlling CPS. However, in addition to restating the terms of the CPS, the RPA may also contain language whereby the relying party acknowledges that he has: access to sufficient information to make an informed decision to rely; agreed to be bound by the terms of the CPS; and, is solely responsible for deciding whether to rely on a certificate. Thereafter, should a party suffer damages as a result of the reliance that bound them to the RPA, the terms of the RPA govern the availability and type of recourse against the CA.

Through the provisions of the CPS and RPA, a CA unilaterally sets the minimum standards and maximum limits of its liability. Unless a digital signature statute states the contrary, these self-imposed standards and limits control the relationship between the CA and relying party. In addition, the language of the CPS and RPA dictates the kinds and amounts of damages an injured relying party may recover. Asserting a claim against a CA pursuant to these agreements involves different common law and contract theories.

[93] *See* Wu, *supra* note 90, at 326.

C. Enforcing the Liability Standards: Making a Claim for Damages Against a CA

If a CA fails to follow the standards required by statute or as prescribed in its CPS, it can be liable for damages. The manner of recovery against a CA will depend upon whether the CA is governed by a statute that contains provisions relating to the liability of the CA, or whether the CA's activities are governed by agreement of the parties. Even if statutory provisions exist, there may be no set mechanism for recovery such as a guaranty or letter of credit.

Currently, only three statutes regulating CAs require a CA to maintain a minimum guarantee.[94] This guarantee protects relying parties by ensuring the availability of funds to offset a financial loss suffered by them. However, the ability to recover against a guarantee is not absolute.

While a guarantee provides further assurance to the relying party that the CA has the ability to reimburse him, the relying party can only recover up to the maximum limit on the guarantee. Moreover, the combined aggregate liability of the CA for all claims cannot exceed the maximum limit of the guarantee. Therefore, three claims of loss under the same certificate, or multiple certificates, for $15,000 against a $30,000 guarantee will result in the claimants recovering less than the full amount of their damages. In those states that require no guarantee or bond be maintained by the CA, the relying party must bring a separate civil action against the CA.

Absent a guarantee, an injured party must bring a civil action against the CA in order to recover its losses. If laws of Utah, Washington, Minnesota, or Illinois, as described above, govern the transaction, the injured recipient will have a statutorily enacted liability standard to utilize. If not, the injured recipient must look to the terms of the CPS, RPA, or other agreement that governs the digital transaction. In that case, the recipient is most likely to assert a claim for negligent misrepresentation, breach of written contract and/or breach of implied contract.[95]

IV. CONCLUSION

Currently, statutory provisions exist that provide for limited financial responsibility of CA's for damages caused by reliance on a certificate. However, the law is neither uniform nor complete across the United States. States must continue to develop digital signature legislation that will ensure the authenticity and reliability of electronic messages and

[94] *See* UTAH STAT. ANN. § 46-3-201 (West Supp. 1997); WASH. STAT. ANN. § 19.34.200 (1997); and MINN. STAT. ANN. § 325K.05 Subd. 1(4) (West Supp. 1998).

[95] *See* Wu, *supra* note 90, at 326.

protect the consumers of those messages. Absent uniform and countrywide legislation, the financial responsibility of CA's will continue to be determined mostly by contract. This allows CA's to limit their responsibility through contracts that they themselves create and which relying parties may be unaware of or unable to modify.

Relying parties need to be aware that they may recover damages against a CA based on reasonable reliance on a certificate. However, limits to their reliance exist under both statute and contract that could significantly affect their ability to recover the full amount of reliance damages. In addition, relying parties must be aware not only of the limitations on recovery, but also of the presence or absence of state mandated recovery mechanisms. Absent a suitable bond or guarantee, a CA may be financially unable to satisfy a judgment for damages. Therefore, it is critical that a potential relying party be satisfied with the assurances of trustworthiness of the CA and have full knowledge of the terms that govern his or her reliance.

The decision to rely on a particular certificate rests solely on the recipient. Even when transacting business with a known subscriber, the possibility of fraud exists. Therefore, whether transacting business with a known or unknown subscriber, and a known or unknown CA, a recipient should take all necessary precautions to ensure the validity of the digital transaction. Should a recipient choose to rely on a certificate and complete the digital transaction, he should rely on the digital signature only to the extent that the total amount of risk is not greater than the reliance limit of the certificate. He will thereby protect his ability to recover the full amount of damages he may incur as a result of an error or fraud in the transaction.