UIC John Marshall Journal of Information Technology & Privacy Law

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

Article 11

Spring 1999

A Proposed Code of Professional Responsibility for Certification Authorities, 17 J. Marshall J. Computer & Info. L. 1003 (1999)

Dina Athanasopoulos-Arvanitakis

Marilynn J. Dye

A PROPOSED CODE OF PROFESSIONAL RESPONSIBILITY FOR CERTIFICATION AUTHORITIES

by DINA ATHANASOPOULOS-ARVANITAKIS† & MARILYNN J. DYE††

I. INTRODUCTION

Purpose of the Code:

The purpose of this Code is to guide certification authorities[1] with sound standards for authenticating international computer-based transactions[2] when statutes, signature acts, or other official directives remain silent. As a supplement to developing legislative regulations[3] it is intended that the Code will help elevate the Certification Authority's office

† LL.M., June 1999, The John Marshall Law School. B.A., University of Chicago; J.D., The John Marshall Law School. I dedicate this to my family, whose love and support have been the driving force behind all of my achievements.

†† LL.M. Candidate, June 1999, The John Marshall Law School. Notary Public, State of Illinois. B.S.G.S., Northwestern University; J.D., The John Marshall Law School.

1. The term "Certification Authorities" shall be used in this article to describe persons who perform the tasks of "cybernotarizations." Michael L. Closen & R. Jason Richards, *Notaries Public – Lost in Cyberspace or Key Business Professionals of the Future?*, 15 J. MARSHALL J. OF COMPUTER & INFO. L. 703, 704 n.6 (1997). The American Bar Association coined the phrase "cybernotary" to describe persons who perform the tasks related to the certification and authentication of e-commerce. *Id.* citing John C. Yates, *Recent Legal Issues in Electronic Commerce and Electronic Data Interchange,* 430 PLI/PAT 271, 300 (1996).

2. Computer-based transactions or e-commerce can generate real benefits as it is predicted that Internet business-to-business trade will grow to $327 billion by the year 2002. Nikki Goth Itoi, *Web Sites That Sell*, HEMISPHERES, Nov. 1998, at 60, 62.

3. For a list of states and countries that have pending and enacted legislation governing cybernotarizations, electronic signatures or digital signatures, see Closen & Richards, *supra* note 1, at 715 n.69 (listing AZ, CA, CT, DE, FL, GA, HI, IL, IA, LA, MA, MI, MN, NM, NY, OR, RI, UT, VA, WA, and WY) (citing Shinichi Tsuchiya, *A Comparative Study of the System and Function of the Notary Public in Japan and the United States*, NAT'L NOTARY ASS'N, Jan. 1997 (stating that Japan, German and Chile are also considering digital signature legislation)). *See also* Information Security Committee, Electronic Commerce Division, Digital Signature Guidelines, 1996 A.B.A. SEC. SCI. & TECH. [hereinafter *Digital Signature Guidelines].*

to a level of professionalism that will not only earn respect, but will also gain foreign recognition and harmonization.[4]

Similar to the notarial office of foreign nations, certification authorities in a position of public officers, and in so acting, are placed "in a position of public trust."[5] Certification authorities are also described as "trusted third part[ies]."[6] Unlike the Notarial office, the office of the Certification Authority is highly technical and demands extensive skill and understanding of trusted systems[7] in order to facilitate and secure electronic commerce by means of computerized communications.[8] Thus, certification authorities, in their role as public officials, are "absolutely vital to both commerce and government."[9] With the approach of the next millennium and the technical demands of advancing technology, the importance of the certification authority's role as public officials has increased substantially as the trend shifts toward a more "paperless society."[10]

For this reason, the need for establishing clear and unambiguous guidelines is particularly important.[11] To that end, the standards in this

---

4. There is a higher esteem for the foreign notary and the office he represents. This is not so in the United States, which explains why "other nations do not as often approve notarizations originating in the United States." Michael L. Closen, *The Public Official Role of the Notary*, 31 J. MARSHALL L. REV. 651, 700 (1998).

5. *Id.* at 685, (citing Farm Bureau Fin. Co. v. Carney, 605 P.2d 509, 514 (Idaho 1980) (finding that "the notary [is] a public officer in a position of public trust.")).

6. *See Digital Signature Guidelines supra* note 3, at 14 (stating that a certification authority shall be referred to as a trusted third party in most technical standards and in the Guidelines). *See generally* John B. Kennedy & Shoshana R. Davids, *Bartleby the Cryptographer, Legal Profession Prepares for Digital Signatures*, 215 N.Y. L.J. 4 (1996).

7. For a general discussion of trusted systems see Mark Stefik, *Shifting The Possible: How Trusted Systems and Digital Property Rights Challenge Us To Rethink Digital Publishing*, (visited Oct. 13, 1998) <http://www.law.berkeley.edu/journal/btjl/articles/12-1/stefik.html> (stating that in the context of digital works, a trusted system follows rules governing the terms, conditions and fees for using digital works).

8. *See Digital Signature Guidelines, supra* note 3, at 14-15.

9. *See* Closen, *supra* note 4, at 701.

10. The concept of a paperless society is becoming a reality with the advancement of computer technology and accessibility to the Internet. *See* Chris Reed, *Authenticating Electronic Mail Messages - Some Evidential Problems*, IV SOFTWARE L. J. 161 (1991).

> [M]ost modern computer systems are able to transmit these documents to another computer through a public telecommunications network. The document, when received, does not need to be printed out but can be stored on disk and retrieved as and when necessary. Apart from the increased efficiency in storage and retrieval that is made possible by this method of communication, there are further advantaged, such as the ability to negotiation the contents of the document by amending and re-transmitting it without the need to retype it from scratch each time.

Id.

11. *See* NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY 1 (Nat'l Notary Ass'n, Semifinal Draft 1998), (describing the need for Notary Publics to adhere to a professional code of conduct). To that end, Certification Authorities, as notaries in cyberspace, should also consider adhering to a code of professional responsibility.

Code were drafted to guide and navigate certification authorities through new and seemingly uncharted territory.[12] By delineating standards, this Code sets out to help certification authorities avoid conflicts, set qualification standards that are akin to foreign standards and promote the integrity of the CyberNotary office.

Organization of the Code:

This Code of professional responsibility is based upon 10 "Guiding Principles"[13] that clarify and describe multiple standards for certification authorities. Each guiding principle is broken down in related subparts that are described as "directives." Each guiding principle will be followed by commentaries explaining the drafters' views, concerns, rationales and justifications in selecting each provision. These commentaries may also discuss other related issues not directly addressed by the Code.

However, codes of ethics and professional responsibility are not rules of "ethics" in the philosophical sense, nor are they rules of morals. The purpose of the codes of ethics and professional responsibility is not to direct public officers that they have to be good, honest, moral people, but to impose rules of conduct and practice on a profession.[14] In most cases, standards do not carry the force of law.[15] Thus, throughout this Code, the word "shall" does not necessarily denote a legal obligation for the certification authority; instead, it always constitutes a compelling recommendation.[16]

Basis of the Code

Presently, there is no "official" Code of Professional Responsibility for certification authorities. In fact, very few states have passed a Digital Signature Act.[17] This is a new field and a constant reminder of how

12. For a general discussion on the topic of the emerging field of notaries in cyberspace, see Victoria Slind-Flor, *Moving Into Cyberspace as Notaries, The Need to Authenticate Electronic Documents Is a New Frontier For Attorneys*, 18 NAT. L.J. 16 (1995).

13. In an attempt to maintain a sense of uniformity in the field of notaries, the authors of this article have assimilated the ten-point format of the NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, as an applicable model for this *Proposed Code Of Professional Responsibility for Certification Authorities*. *See generally* NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11.

14. There are many other professions that also have published codes of ethics. ENCYCLOPEDIA OF APPLIED ETHICS, Vol. 4, at 593 (1998). The Encyclopedia lists not only specific codes of ethics, but breaks the subject of ethics down by: business and economics, concepts, dentistry, education, environmental, journalism, legal, media, medical, policies, politics, scientific, social ethics, social services, sports organizations and theories of ethics.

15. *See* NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 3.

16. *Id.*

17. *See* Closen & Richards, *supra* note 1. For an overview of the current U.S. and International Digital Signature Act, see *Summary of Electronic Commerce and Digital Signature Legislations* (last modified December 1, 1998) <http://www.mbc.com/dssum.html>.

hard it is for the law to keep up with the pace of emerging new technologies.

These Guiding Principles were created with an eye towards the signature acts of Utah,[18] Florida and other states, as well as other codes of professional responsibility. These include, but are not limited to, the Notary Public Code of Professional Responsibility, the Digital Signature Guidelines, and The American Bar Association's Codes of Professional Conduct for both attorneys and judges.[19]

Uses and Benefits of the Code:

The implementation of these guidelines will help promote security and trust in the certification authority's ability to authenticate international computer-based transactions. By requiring certification authorities to be licensed attorneys[20] with a technical background and by imposing a duty of care to the clients and setting stricter standards, it is possible to provide a more secure environment for electronic commerce.[21] More specifically, these standards will help deter fraud and litigation by securing computer-based signatures, which will "(1) minimize the incidence of electronic forgeries, (2) enable and foster the reliable authentication of documents in computer form, (3) facilitate commerce by means of computerized communications, and (4) give legal effect to the general import of the technical standards for authentication of computerized messages."[22]

---

18. Utah is the pioneer in the passing of a digital signature act. *See* S.R. 188 and S.B. 73, 52d Leg. (Utah 1966) (amending UTAH CODE ANN. §§ 46-1-1 to -19 (Supp. 1996) ("Utah Digital Signature Act")).

19. *See* Florida Electronic Signature Act of 1996, FLA. STAT. ANN. § 282.70-75 (West 1996); NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11; DIGITAL SIGNATURES GUIDELINES, *supra* note 3; MODEL CODE OF PROFESSIONAL RESPONSIBILITY (1980); MODEL RULES OF PROFESSIONAL CONDUCT (1983); MODEL CODE OF JUDICIAL CONDUCT (1984).

20. The practice of law requires a license in all 50 States. A license is needed to make appearances in court, take depositions and negotiate settlements. *See* MODEL RULES OF PROFESSIONAL CONDUCT Rule 5.5 (1983).

21. *Digital Signature Guidelines supra* note 3, at 17.

> Digital signatures, if properly implemented and utilized offer promising solutions to the problem of:
>
> • IMPOSTORS, by minimizing the risk of dealing with impostures or persons who attempt to escape responsibility by claiming to have been impersonated;
>
> • MESSAGE INTEGRITY, by minimizing the risk of undetected message tampering and forgery, and of false claims that the message was altered after it was sent;
>
> • FORMAL LEGAL REQUIREMENTS, by strengthening the view that legal requirements of form, such as writing, signature, and an original document, are satisfied, since digital signatures are functionally on par with, or superior to paper forms; and
>
> • OPEN SYSTEMS, by retaining a high degree of information security, even for information sent over open, insecure, but inexpensive and widely used channels.

Id.

22. *Id.* at 18.

This Code will also harmonize the United States' standards for certification authorities and the Notarial Office with the more rigid standards of other countries. By making the United States' standards more comparable to foreign standards, foreign countries will recognize U.S. certified documents as being credible and reliable. Inevitably, the harmonization of certification standards will expedite and encourage growth in electronic commerce. Furthermore, widespread adherence by certification authorities in the United States to these standards will engender heightened respect and recognition for their notarial office in the enterprises of government and business, both in this nation and abroad.[23]

This Code also seeks to promote equal treatment for all people seeking certificates[24] from the certification authority. These principles derive from the conviction that a certification authority, as a public officer, in a democracy must serve all persons equally and be blind to such distinctions as race, nationality, ethnicity, citizenship, religion, politics, lifestyle, age, disability, gender, or sexual orientation.[25]

Finally, this Code may be used as a guiding tool to educate, not only certification authorities, but also Notaries Public, lawmakers, public administrators, and any users of notarial services.[26]

Revision of the Code:

The Proposed Code of Professional Responsibility for certification authorities is meant to be an organic document. This Code is not meant to be static nor set in stone. Its organization is suitable to addition, deletions and amendments with little or no disruption of other guidelines in the Code. Its authors anticipate needed revisions or supplements to accommodate technological and legal developments. Periodic review and revision of this Code is encouraged.

---

23. *See Digital Signature Guidelines, supra* note 3, at 4.

24. "A Certificate is a message which at least (1) identifies the certification authority issuing it, (2) names and identifies the subscriber, (3) contains the subscriber's public key, (4) identifies its operation period and is digitally signed by the certification authority issuing it." *Id.* at 29. "A notary's principle duty involves authenticating a written instrument by attaching his official [acknowledgment] certificate." *Id. See also* Raymond C. Rothman, NOTARY PUBLIC PRACTICES & GLOSSARY, at 15-17 (1978) (stating that "the word 'acknowledgment' is used to mean a 'certificate of acknowledgment,' which is a written statement signed by a Notary). Acknowledgment is also used to man an 'act of acknowledgment,' which is the act of recognition, or admission of the existence, of an agreement made by the party whose signature is notarized. *Id.*.

25. *Id.*

26. *Id.*

II. GUIDING PRINCIPLE I

A. THE CERTIFICATION AUTHORITY IS A LICENSED ATTORNEY WHO HAS THE DUTY TO BE COMPETENT

I-A: THE CERTIFICATION AUTHORITY SHALL BE A LICENSED ATTORNEY.[27]

Directive:

The certification authority is a licensed attorney who bears the responsibility of advising and facilitating notarizations for digital signers[28] who conduct on-line interstate and international transactions.

I-B: THE CERTIFICATION AUTHORITY SHALL BE LICENSED IN INFORMATION TECHNOLOGY.

Directive:

The certification authority is an attorney with an in-depth technical background in computer operations as well as the function of the Internet.[29] The certification authority must command the technical knowledge and expertise to perform secured electronic notarizations through the use of trusted systems and encryption technology.

---

27. Survey by Dina Athanasopoulous and Marilynn J. Dye, authors, (Nov. 1, 1998) (on file with authors). The survey was based on a one-page questionnaire mailed to 25 notary officials in the month of Nov. 1998 with five queries: "(1) Do you think Certification Authorities should be an attorney? (2) Do you think there should be a licensing exam for Certification Authorities? (3) Do you think Certification Authorities are fiduciaries to their clients? (4) Do you think Certification Authorities should be required to take continuing education coursed on information systems technology? (5) Do you think Certification Authorities should be allowed to notarize their own transactions?" To questions (1) 70 percent responded in the affirmative.

28. "A digital signature is a transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and a signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds tot he signer's public key, and (2) whether the initial message has been altered since the transformation was made." *See Digital Signature Guidelines, supra* note 3, at 35. "The term 'electronic signature' is generally used with a meaning including all legally recognizable signatures under the current definitions of 'signature.' *See, e.g.,* U.C.C. § 1-201 (39) (1990). An 'electronic signature' thus includes digital signatures a defined by the Digital Signature Guidelines. Electronic signatures also include digitized images of paper-based signatures, typed notations such as "s/Tim Smith", and perhaps addressing information such as the "From" headers in electronic mail." *Id.* A signer is a person who creates a digital signature for a message. *Id. at 50.*

29. The Internet can be described as a decentralized, global communications medium linking people, institutions, corporations, and governments all across the world. *See* ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa.), *prob. juris. noted,* 117 S. Ct. 554 (1996). Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996). The Internet is a network of networks – a decentralized, self-maintaining series of redundant links among computers and networks, capable of rapidly transmitting communications without direct human control or involvement. AKA v. Pataki, 969 F.Supp. 160, 164 (1997). For a more thorough discussion of the origins of the Internet, see *A Brief History Of the Internet,* (visited Aug. 22, 1998) <http://www.isoc.org/internet-history/brief.html>.

I-C: THE CERTIFICATION AUTHORITY SHALL UPDATE AND CONTINUE HIS EDUCATION IN INFORMATION TECHNOLOGY.

Directive:

The certification authority shall remain current on the latest computer technology used to secure electronic data certification. The certification authority is encouraged to take continuing education[30] and supplemental training classes on the latest encryption technology and any other developments that affect the performance of cybernotarization.

I-D: THE CERTIFICATION AUTHORITY SHALL BE COMPETENT AT ALL TIMES.

Directive:

The certification authority shall be able and competent in order to certify digital and electronic transactions.

B. COMMENTARY—GUIDING PRINCIPLE I

General Comments:

Guiding Principle I sets the tone for the entire Code. By requiring the certification authority to be a licensed attorney with a strong technical background in information technology, the Principle makes it clear that the certification authority will be in a position of heightened responsibility and, consequently, prestige."[31]

Certification authorities must possess the integrity necessary to conduct on-line interstate and international transactions, which because of their nature, are usually of greater value and consequence than everyday transactions.[32] A certification authority's function will include the guaranteeing of transactions. "In a high stakes deal, the parties may prefer to know not only that the signature is authentic, but that the contract itself is valid."[33] Thus, certification authorities should be required to have a "good understanding of Contract law, international law, as well as computer and telecommunications technology in general."[34] For these reasons, only attorneys licensed in information technology should fill the role of certification authority.[35]

---

30. *See* Survey, *supra* note 27 (stating that in response to question (4) of those surveyed 100 percent responded that a Certification Authority should be required to take continuing education coursed on information systems technology).

31. Glen-Peter Ahlers, Sr., *The Impact of Technology on the Notary Process*, 31 J. Marshall L. Rev. 911, 920 n. 44 (1998). *See also* Margaret A. Jacobs, *Will Notaries Still Reign Over Red Tape When Documents Move Electronically?*, WALL ST. J., Mar. 12, 1996, at B1 (stating that Cybernotaries will combine both legal and computer expertise to verify the authenticity of electronic documents produced in cyberspace).

32. *Id.*

33. *See* Closen & Richards, *supra* note 1, at 740.

34. *Id.*

35. *See* Ahlers, *supra* note 31.

Furthermore, certification authorities who possess elevated levels of expertise will play a critical role in facilitating business and electronic commerce on the Internet. By requiring certification authorities to be licensed attorneys who have an in-depth knowledge of trust systems and encryption technology, there will be more secured transactions and greater confidence in those transactions. "The channels of commerce are rapidly being filled with computerized messages. Secure electronic commerce increasingly depends upon securing the information itself, rather than relying upon the security of the channel. Modern cryptography[36] can make information safe from eavesdropping, tampering, or forgery, regardless of the security of a communication channel. Cryptographic technology[37] can also authenticate a message by assuredly linking it to an identified person and guarding the message's integrity."[38]

> Secure electronic records and secure electronic signatures define categories of records and signatures that are accorded heightened evidentiary presumptions because of their enhanced reliability and trustworthiness, just as notarized documents are accorded heightened evidentiary presumptions for the same reason. The concept of a secure electronic record and a secure electronic signature is critical to enabling electronic commerce. Businesses will be much more willing to enter into commercial transactions, extending credit, commit resources, ship goods, or otherwise rely on messages from contracting parties transmitted over public networks such as the Internet when they can be assured that such records and signatures will be accorded the heightened eviden-

---

36. *See* Stewart A. Baker, *Decoding OECD Guidelines for Cryptography Policy*, 31 THE INTERNATIONAL LAWYER 729 (1997) (stating cryptography can also authenticate a document (or some other piece of data) and using cryptography to ensure data integrity allows a person receiving a message to confirm that the message has not been altered in transit).

> Cryptography is a means of putting data in code. It allows people to transform a message or data into a form that can't be understood (decrypted) without knowledge of some secret information. A user who wants to encrypt a message applies a mathematical function, called an algorithm, in order to scramble the message. The algorithm allows the user to select an individual 'key.' The algorithm then uses the key to encrypt the message. After the user sends the encrypted message, the recipient applies the same algorithm to decrypt the message. For a given algorithm, the strength of the cryptography increases with the length of the key, which is measured in bits.

Id. *See also* Reed, *supra* note 10, at 1169 (stating that cryptography is becoming increasingly popular as the method of ensuring the security of messages against unauthorized interception).

37. The most commonly used cryptographic technology system is the Data Encryption Standard (DES). DES is a complicated form of encryption. In simple terms, DES depends on a 64-bit key (K) known only to the sender and recipient. *Id.*

38. For a through discussion of cryptography, encryption and digital signatures, see *generally* Jeff Prosise, *Digital Signatures: How They Work* (visited April 9, 1996) <http://www.zdnet.com/pcmag/issues/1507/pcmg0090.html>. The term cryptography implies encryption, but cryptography is not limited to theories of data encryption. It also addresses issues that are related to digital authenticity – how you know that the electronic data is real and how electronic documents can be "signed". *Id.*

tiary presumptions necessary to effectively make their transactions nonrepudiable.[39]

Finally, by requiring certification authorities to be attorneys with formal knowledge of encryption technologies, foreign countries will more readily recognize and acknowledge the certificates that U.S. certification authorities will issue. Foreign recognition and respect will impact and promote business and electronic commerce[40] on an international level. Presently, "the United States tends to give effect to notarizations of many other countries because their notaries tend to be more highly educated, trained, authorized and respected than our notaries."[41] Thus, there is a higher esteem for the foreign notary and the office he or she represents. This is not so in the United States, which explains why "other nations do not as often approve notarizations originating in the United States."[42] "The significant discrepancies between the notaries in the United States and the notaries operating in foreign nations has created the atmosphere in which foreign recipients of notarial acts per-

39. Ill. Attorney General Jim Ryan's Comm. on Elec. Commerce and Crime, 90th Sess., *Final Report of the Comm. on Elec. Commerce and Crime* (visited May 8, 1999) <http://www.mbc.com/legis/cecc-fin.html> [hereinafter *Final Report of the Comm. on Elec. Commerce and Crime*].

40. Electronic commerce means: a paperless process including electronic mail, electronic bulletin boards, electronic funds transfer, electronic data interchange, and similar techniques for accomplishing business transactions. The use of terms commonly associated with paper transactions (*e.g.* 'copy', 'document', 'page', 'printed', 'sealed envelope' and 'stamped') shall be interpreted to restrict the use of electronic commerce. 48 C.F.R. § 4.501. *See also* Itoi, *supra* note 2.

41. The approximately 4.2 million American notary population is a sharp contrast to the notary population of other countries, such as Japan and Latin America. *See* Closen, *supra* note 4, at 699 ("In most jurisdictions of Central and South America and in Puerto Rico, only lawyers can also occupy the position of *notario publico*. The *notario publico*, the Japanese *koshonin*, and the French *notaire* all possess vastly greater authority than our notaries."). In comparison to the millions of U.S. notaries, Japan has only approximately 550. *Id.* The combination of minimum formalities, easy access and low qualification standards explains why there is such an excessive amount of notaries in the U.S. today. This combination and the overflow of notaries have generated apathy and indifference towards the special status of the notary office. *See* Milton G. Valera, *The National Notary Association: A historical Profile*, 31 J. MARSHALL L. REV. 971, 997 (1998) ("[T]he ranks of notaries are plagued by apathy and indifference toward their role. This situation is made worse by the fact that notary programs in most states perennially struggle with lack of funds to appropriately inspire, educate, and update their notaries."). Even the U.S. Supreme Court has commented on this phenomena: "the significance of the position has necessarily been diluted by changes in the appointment process and by the wholesale proliferation of notaries." *See* Karla J. Elliott, *The Notarial Seal – The Last Vestige of Notaries Past*, 31 J. MARSHALL L. REV. 903, 907 n.40 (1998) (citing *Bernal v. Fainter*, 467 U.S. 216, 224 n.12 (1984)).

42. *See* Closen, *supra* note 4, at 700.

formed in the United States accord such acts little or no credibility."[43]

The higher standards imposed on the certification authority are necessary curative actions since "the disparity of the notary status in the international arena is a serious issue that must be addressed. Commercial transactions will suffer if foreign businessmen and lawyers continue to look askance at our notarizations."[44] This Guiding Principle is an attempt to ameliorate some of these problems by setting higher standards that are more comparable and uniform with international standards. Moreover, this Principle promotes domestic and international confidence in the integrity and reliability of electronic records and electronic commerce.[45]

C. ARTICLE A: THE CERTIFICATION AUTHORITY SHALL BE A LICENSED ATTORNEY

A certification authority is a "trusted third party" whose principle function is to bind a key pair with the identity of a person who is to sign, termed a "subscriber."[46] To associate a key pair with a subscriber, a certification authority issues a certificate, an electronic record that lists a public key as the "subject" of the certificate and confirms that the subscriber identified in the certificate holds the corresponding private key.[47] The certification authority performs this process by using trustworthy systems (defined and discussed more fully in Article B).

To perform this function, "quality assurance should be a principle concern in selecting and utilizing [c]ertification [a]uthorities."[48] To ensure quality assurance, "[c]ertification [a]uthorities [a.k.a. cybernotaries] are attorneys at law admitted to practice in the United States and qualified to act as a CyberNotary pursuant to specialization rules currently under development in the CyberNotary Committee, Section of Science and Technology of the American Bar Association."[49] "A cybernotary's

43. Keith D. Sherry, *Old Treaties Never Die, They Just Lose Their Teeth: Authentication Needs of a Global Community Demand Retirement of the Hague Public Documents Convention*, 31 J. MARSHALL L. REV. 1045, 1049-50 (1998) citing Michael L. Closen, *Why Notaries Get Little Respect,* NATIONAL L. J., Oct. 9, 1995, at A24.

44. *See* Ahlers, *supra* note 31, at 921.

45. *See* ILLINOIS ELECTRONIC COMMERCE SECURITY ACT, *supra* note 39, at 11.

46. "A Subscriber is defined as a person who (1) is the subject named or identified in a certificate issued to such a person, and (2) holds a private key that corresponds to a public key listed in that certificate." *Digital Signature Guidelines, supra* note 3, at 14.

47. "A person seeking to verify a digital signature needs, at minimum, (1) the public key corresponding to the private key used to create the digital signature, and (2) reliable evidence that the public key (and thus the corresponding private key of the key pair) is identified with the signer. The basic purpose of the certificate is to serve both the needs in a reliable manner." *Id.*

48. *See Digital Signature Guidelines, supra* note 3, at 31, cmt. 1.6.1.

49. *Id.*

function mirrors that of a notary, and is focused primarily on practice in international, computer-based transaction."[50] "It is proposed that a CyberNotary would be required to meet a level of qualification as a legal professional commensurate with that of notary, be a member of good standing of the bar of a state or territory of the United States, be a member of the American Bar Association, and demonstrate technical competence in computer-based business transactions."[51]

However, in addition to assuring the validity of a digital signature,[52] certification authorities [or cybernotaries] also provide important "ancillary services."[53] For example, "a notarial authentication in certain legal systems assures the validity and legal efficacy of the transaction itself, not merely its signatures."[54] The certification process itself is a legal process since "a certification practice statement may also be comprised of multiple documents, a combination of public law, private contract, and/or declaration."[55] Furthermore, a certification authority may be called upon to render advice on a particular transaction in a given matter involving a notarial act or provide particular documents required for a particular transaction. Other ancillary services regarding areas of generally accepted security principles that a certification authority may provide include, but is not limited to, providing archival, confirmation, directory, technical due diligence, financial assurance, key pair generation, message corroboration, time-stamping, and commercial key escrow services.[56] Hence, there are compelling reasons why certification authorities should be attorneys.

D. ARTICLE B: THE CERTIFICATION AUTHORITY SHALL BE LICENSED IN INFORMATION TECHNOLOGY

A certification authority possesses "technical expertise to facilitate computer-based transactions requiring a high level of certification, authentication, or other information security services."[57] A certification

50. *Id.*

51. *Id.*

52. "Digital signatures are a principal way to authenticate the identities of the parties in electronic commercial transaction, such as e-mail purchase orders or electronic funds transfers." Baker, *supra* note 32, at 730.

53. Ancillary service is 1) a person offering or performing a service, other than issuance of a certificate, in support of digital signatures and other related areas of secure electronic commerce, or 2) the service offered or performed by such person. Secure electronic commerce is the establishment of a system/infrastructure/method of communication such that transactions can be relied upon. *See Digital Signature Guidelines*, *supra* note 3, at 23.

54. *See Digital Signature Guidelines*, *supra* note 3, at 31.

55. *See id.* at 33.

56. *See id.* at 24-26 (providing a more in depth discussion of Certification Authority ancillary services).

57. *Id.* at 31.

authority performs two essential functions. First, he or she is responsible for identifying and authenticating the intended subscriber to be named in the certificate, and verifying that such subscriber possesses the private key that corresponds to the public key[58] that will be listed in the certificate. Second, the certification authority is responsible for creating and digitizing the certificate. The certificate issued by the certification authority represents that the certification authority's statement as to the identity of the person named in the certificate and the binding of that person to a particular public-private key pair.[59]

The issuance of this certificate is a security procedure. In order to issue a certificate, the certification authority must use trustworthy systems.[60] The Digital Signature Guidelines defines "trustworthy systems" as "computer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonably reliable level of availability, reliability and correct operation; (3) and reasonably suited to performing their intended functions; and (4) adhere to generally accepted security principles."[61] Trustworthy systems incorporate security procedures that may require the use of algorithms or codes,

---

58. *See* Baker, *supra* note 36, at 730

> An algorithm can be either a secret key [or "private key"] algorithm or a "public key" algorithm. In a [private] key algorithm, the same key is used for encrypting and decrypting. The advantage of a [private] key algorithm is that is can provide very good security and does not take a lot of time to encrypt and decrypt data. [A] [private] key algorithm . . . requires the sender and the receiver to decide on the key – and to share it securely – before they can send an encrypted message.
>
> A public key algorithm, the key used for encrypting is different from the key used for decrypting. Therefore, one of the keys can be made public. For example, one of the keys could be listed in a directory of users. This listing allows a complete stranger to send an encrypted message to anyone in the directory. The recipient can then use his or her private decryption key to read the message. The advantage of a public key algorithm is that correspondents who have never shared a single secret key in advance can exchange secure message easily).

Id.

Baker describes the process by "[t]he sender encrypts the information with his or her private key, thereby signing the document, and sends the information to the recipient. The recipient decrypts the information wit the sender's public key thereby verify that the document indeed cam from the sender." *Id.* at 730-31. *See also* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 573 (stating that Public key cryptography is a classic example of a privacy-enhancing technology). This technology allows the contents of information to be secured against unauthorized access). *Id.*

59. Currently there are companies like VeriSign Inc. of Mountain View, Calif. that issues digital certificates, that certify the identity of people and companies that use digital signatures. Don Clark, *Safety First,* WALL ST. J., Dec. 7, 1998, at R14. These companies "tap features in Web browser software that can recognize digital signatures and help protect transactions with little extra work from consumers." *Id.*

60. *See generally* Stefik, *supra* note 7.

61. *See Digital Signature Guidelines, supra* note 3, at 54.

identifying words or numbers, encryption, answer back or acknowledgment procedures, or similar security devices.

The implementation of trustworthy systems satisfies certain objectives. First, trustworthy systems promote confidentiality by ensuring that sensitive information is not disclosed or revealed to unauthorized persons. Second, trust systems promote integrity in the certification process by ensuring consistency of data; in particular, the prevention of unauthorized creation, alteration, or destruction of data. Third, trust systems promote availability by ensuring that legitimate users are not unduly denied access to information and resources. Fourth, trust systems promote legitimate use by ensuring that only authorized persons use resources in authorized ways.[62]

Essentially in a trusted system, computers talk to each other to establish that they are both trusted systems and to determine their security levels and billing methods.[63] "One way to do this is with a challenges response protocol. This protocol is similar to what you might imagine in a 'spy versus spy' scenario when two secret agents who are strangers to one another first meet."[64] The security of computer communications relies on the use of public key cryptography.[65] Basically, in public key systems, there are two keys used by a system for encryption: a public key and a private key. Each computer keeps its private key secret and its public key known or listed in a directory. The keys are inverses (mathematically related). Anything encrypted in the public key can be decrypted by the private key and, therefore, anything encrypted in the private key can be decrypted by the public key. It is imperative to have the proper key for decoding a message.

---

62. [T]he design, implementation, and maintenance of trustworthy system should include measures: -to prevent unauthorized access to or use if the system, especially of its private key, and particularly a certification authority's private key used in issuing certificates; - to arrange personal duties, access restrictions, and internal auditing procedures such that the system's security and operation cannot be compromised through the efforts of any single person having an interest in the outcome of system operations, or in collusion with other persons having an interest in the outcome of system operations; - to provide fail safes and procedures designed to minimize consequences, should a primary security measure fail; - to reduce the effects of natural disasters and other forces majeures, as well as the risk of financial difficulties, sabotage, employee infidelity, and other foreseeable events; - to maintain an audible record of its services separately and independent of from its operative system.

Id. at 55.

63. *See generally* Stefik, *supra* note 7.

64. *Id.*

65. "Cryptography allows the recipient of information to confirm that the information came from a certain sender (*i.e.* that the message is not a forgery). Authentication can prevent later repudiation: if the message is confirmed as authentic, the sender cannot easily deny that he or she sent the message." Baker, *supra* note 32, at 730.

The certification authority relies on trust systems to associate a key pair with a prospective signer. To perform this function, "the certification authority issues a certificate, an electronic record which lists a public key as the subject of the certificate, and confirms that the prospective signer identified in the certificate holds the corresponding private key."[66] After the certification authority issues a certificate, the certification authority digitally signs the certificate. The digital signature assures both message and identity[67] authenticity of the certificate.[68] Digital signature depends on encryption technology:

> [e]ncryption technology[69] allows one not only to encode a message, but also to apply a digital signature to the document, which is encoded. While the digital message might be interpreted by others, only the [c]ertification [a]uthority holding the correct key can unwrap the signature package to verify the signature, unwrap the encoded message, and verify that the contents of the original package have not been tampered with since being sent into the electronic stream.[70]

The level of the trust system's security is a matter of degree.[71] The level of security depends on the type of transaction involved.[72] Security procedures are broad enough to include not only encryption technology, but other technologies in place today, as well as new technologies that will be developed in the future. For instance, the certification authority may choose to implement teleconferencing technology as a supplement to encryption technology as a means to further guard against fraud.

> One way to accomplish this task might be to electronically capture the signing of an agreement, digitally signing the video in a manner that shows the parties entering into the transaction, and simultaneously locking the image so that any tampering would be detected. . . . The computer could also capture the visual portion of the meeting when the counselors all agreed to the transaction, and digitally wrap the video

---

66. *See Digital Signature Guidelines*, *supra* note 3, at 14.

67. For a discussion of identity in Cyberspace see John Browning, *I Encrypt, Therefor I Am* (visited Nov. 1977) <http://www.wired.com/wired/archive.tizen.html>.

68. [T]he issuing certification authority's digital signature on the certificate can be verified by using the public key of the certification authority listed in another certificate by another certification authority, and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness. In each case, the issuing certification authority must digitally sign its own certificate during the operational period of the other certificate used to verify the certification authority's digital signature.

Digital Signature Guidelines, *supra* note 3, at 16.

69. *See* Ahlers, *supra* note 31, at 919.

70. *See id.* at 918.

71. *See Digital Signature Guidelines*, *supra* note 3, at 63, cmt. 3.1.1.

72. *See id.* at 56, cmt. 1.35.3.

portion up with the text.[73]

Hence, an extensive background and thorough understanding of Information Technology is paramount in enabling a certification authority to provide secure electronic records and digital signatures. Secured electronic records and signatures are accorded heightened evidentiary presumptions because of their reliability and inherent trustworthiness.[74] Secured electronic records and secured digital signatures, and the presumptions that flow from that status, are critical in enabling a viable system of electronic commerce. These presumptions give legal assurances to persons engaged in electronic commerce that their transaction documents would be provable and enforceable. Thus, businesses will be more willing to participate in electronic commerce when they can be assured that their records and signatures will be nonrepudiable.[75] Certification authorities are instrumental in this nonrepudiation process. By having the requisite knowledge to properly secure records and signatures, the certification authority will promote trust and confidence in every electronic commercial transaction.

E. Article C: The Certification Authority Shall Update and Continue His Education in Information Technology

To maintain the requisite knowledge and skill, a certification authority should engage in continuing study and education. The certification authority should complete a minimum number of hours of training specifically in cybernotary ethics, law and practice. A recommended course of study is at least 20 hours per year.

Furthermore, there should be some governing body to establish and maintain mandatory programs for certification authorities who seek to renew their commissions, including segments on new developments and

---

73. The cybernotary shall conduct each transaction via teleconferencing. The use of videos will overcome the special problems due to lack of physical presence. The use of videos will also aid the cybernotary to guard against fraud;—since lack of physical presence increases the chances of fraud. *See* Charles N. Faerber, *Being There: The Importance of Physical Presence To the Notary,* 31 J. Marshall L. Rev. 749, 754 (1998). "With electronic notarizations, the notary's byword of *habeas corpus*, 'you have the body', must be replaced by a new motto of *videas corpus*, 'you see the body'." *Id.* at 776. One way to accomplish this task might be to electronically capture the signing of an agreement, digitally signing the video in a manner that shows the parties entering into the transaction, and simultaneously locking the image so that any tampering would be detected. . . .the computer could also capture the visual portion of the meeting when the counselors all agreed to the transaction, and digitally wrap the video portion up with the text. *See* Ahlers, *supra* note 31, at 924.

74. *See Final Report of the Comm. on Elec. Commerce and Crime, supra* note 39, at 7.

75. Including extending credit, commit resources, ship goods and otherwise rely on messages from contracting parties transmitting over the Internet. *See id.*

review of traditional standards.[76] This may include a system of peer review or other types of legal and technological continuing education. In addition, a re-examination of certification authorities' skill shall be performed on a bi-annual basis before renewal of their commissions or licenses.[77]

The requirement of certification authorities to continually educate and test themselves gives rise to two important benefits. Not only will U.S. certification authorities gain foreign recognition and trust, they will also maintain the quality of their performance as certification authorities.[78]

F. ARTICLE D: THE CERTIFICATION AUTHORITY SHALL BE COMPETENT AT ALL TIMES

The certification authority is "able" when he or she possesses the requisite knowledge and technical background and skill to certify electronic and digital transactions. If the certification authority knows or should know that he or she does not poses the requisite knowledge or technical background for a particular transaction, the certification authority shall recuse himself from that transaction and advise the client to seek certification elsewhere.[79] Alternatively, the certification authority may refer his or her client to another certification authority who has the needed experience for a particular transaction.

The certification authority is "competent" when he or she possesses the physical and mental capacity to perform his or her cybernotarization functions. If the certification authority is physically or mentally impaired, the certification authority shall resign his or her commission. For example, if the certification authority's vision is failing, making it too difficult to read electronic messages, read keys or properly identify parties, then the certification authority should resign his or her commission. These are commonsense restrictions that state the obvious and do not need further elaboration. The resigning certification authority shall report his or her resignation to the commissioning agency.

---

76. *See* Closen & Richards, *supra* note 1, at 756 (suggesting that the continuing education programs should include cybernotary ethics, law and practice topics; including a re-examination before a renewal of a commission is granted).

77. *See* Survey, *supra* note 27, (stating in response to question (2) 80 percent of those surveyed believed there should be a licensing exam for Certification Authorities).

78. *See* Closen & Richards, supra note 1 at 756.

79. Not unlike attorneys, Certification Authorities should maintain the integrity and competency of their profession. *See* MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 1 (1980); MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.1 (1983).

III. GUIDING PRINCIPLE II

A. THE CERTIFICATION AUTHORITY HAS INTERNATIONAL JURISDICTION[80]

II-A: THE CERTIFICATION AUTHORITY SHALL BE COMMISSIONED IN EVERY STATE.

Directive:

Once commissioned, the certification authority can issue a certificate in any state in the United States. A certification authority's certificate shall be recognized in every state.

II-B: THE CERTIFICATION AUTHORITY SHALL PASS AN INTERNATIONAL NOTARY EXAM.

Directive:

The certification authority that issues certificates for international business transactions shall pass an international notary exam.

B. COMMENTARY—GUIDING PRINCIPLE II

ARTICLE A: THE CERTIFICATION AUTHORITY SHALL BE COMMISSIONED IN EVERY STATE.

Due to its amorphous nature, it is next to impossible to place boundaries on the Internet. The whole idea of the Internet is to transcend boundaries. Since the certification authority may deal with electronic commerce via the Internet,[81] the certification authority's certificates shall be accorded recognition in every state. This point is best illustrated with an example: suppose that a certification authority is commissioned in State One, but because of some circumstance the certification authority is located in State Two. If the certification authority brings his or her computer to State Two and conducts electronic notarizations and issues certificates in that state, should the certificates be invalidated simply because the certification authority is physically located in another state? The authors opine that it should not make any difference where the certification authority is located at the time he or she performs electronic data certifications. Physical location should be irrelevant because com-

---

80. Information flows on the Internet crossing all state, country and content boarders. The geographical limits of cyberspace have diminishing value, physical boarders become transparent, and legal systems have local relevance. Therefore, Internet activities may make certification authorities and e-commerce users subject to legal rules and multi-jurisdictions. Therefore geographical proximity and physical contact have less relevance in cyberspace. *See* Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace* (visited Dec. 7, 1998) <http://www.law.emory.edu/ELJ/volumes/sum96/reiden.html> (stating that network borders are replacing national borders).

81. "Dirt roads between towns once carried commerce. Railroad tracks and superhighways that spanned continents, and ships that crossed the seas then surpassed the dirt road. Presently, electronic bits of information that instantly travel worldwide on the information highway deliver today's precious commodities." Ahlers, *supra* note 31 at 916-917.

puters communicate over state lines. Thus, the certification authority's certificates shall be valid regardless where they were transacted.

ARTICLE B: THE CERTIFICATION AUTHORITY SHALL PASS AN INTERNATIONAL NOTARY EXAM.

In order to successfully transact international business, cybernotary certification should be structured similarly to the United States Federal Patent Bar. Certification authorities with the requisite legal experience and technical background could sit for an International Notary Exam. "Upon successful completion, a special United States or International Notary Commission would be granted. Such a system might prosper if it gained international support. Then uniform prerequisites, commissioning standards, and testing services sanctioned by an international body could ensure worldwide acceptance of notarial acts."[82]

The requirement that certification authorities be licensed on some common international level is a substantial step towards bridging the gap between the more stringent requirements foreign notaries and the lax requirements notaries enjoy in the United States.

IV. GUIDING PRINCIPLE III

A. THE CERTIFICATION AUTHORITY SHALL BE A FIDUCIARY[83]

III-A: THE CERTIFICATION AUTHORITY SHALL BE A PUBLIC OFFICIAL.[84]

Directive:

The certification authority as a public official owes a fiduciary duty to the public.

III-B: THE CERTIFICATION AUTHORITY SHALL BE A FIDUCIARY TO HIS OR HER SUBSCRIBER AND RELYING THIRD PARTIES.

Directive:

The certification authority shall be a fiduciary to his or her subscriber and/or relying third party as provided by contract or by law. The

82. *See Id.* at 921-922.

83. A Certification Authority should have the same fiduciary duties as a Notary. "As a matter of sound business policy and public policy, notaries should be held to relevant fiduciary standards." Closen *supra* note 4, at 666-667. "Such trust should extend to both the general public as well as the document signer; and in a cybernotary's case—the electronic document signer." *Id.*

84. A notary is a public official empowered by the states to perform specified duties. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 8. As public officials, notaries are authorized to acknowledge, verify upon oath or affirmation, witness and attest as to the validity of a signature and administer an oath or affirmation. Gerald Haberkorn & Julie Z. Wulf, *The Legal Standard of Care for Notaries and Their Employers*, 31 J. MARSHALL L. REV. 735, 737 (1998).

certification authority who provides ancillary services shall also be a fiduciary to his or her client.

B. COMMENTARY—GUIDING PRINCIPLE III

ARTICLE A: THE CERTIFICATION AUTHORITY SHALL BE A FIDUCIARY TO THE PUBLIC.

Notaries are in a profession of public officers and in so acting are placed "in a position of public trust."[85] Similarly, certification authorities, acting as cybernotaries, serve in the same capacity as public officers and are in a position of public trust. Certification authorities serve as agents and fiduciaries[86] of the public, and "may serve as agents and fiduciaries of their employers."[87]

Certification authorities issue certification practice statements.[88] A certification practice statement details the trust systems and practices a certification authority employs in issuing certificates.[89] A certification practice statement may also provide "the details of what is reasonably secure from intrusion and misuse, . . . and a reasonably reliable level of availability."[90] Furthermore,

> a certification practice statement should indicate any of the widely recognized standards to which the [c]ertification [a]uthority's practices

---

85. *See* Closen, supra note 4, at 685 (citing farm Bureau fin. Co. v. Carney, 605 P.2d 509, 514 (Idaho 1980) (finding that "the notary [is] a public officer in a position of public trust")).

86. *See* Closen, *supra* note 4, at 663-664.

> Fiduciary duties arise as the result of one or more parties entrusting property or contract rights to a fiduciary, or as the result of parties entering into a confidential relationship (in which case each party might become a fiduciary of the other). A fiduciary relationship is one exemplified by trust and confidence being reposed by one party (the entruster) in another party, the fiduciary who accepts such responsibilities. Document signers certainly entrust information, sometimes valuable and/or personal information . . . to notaries [or Certification Authorities], especially notaries who maintain journals of notarial activities. A fiduciary is like a trustee, one who is to act primarily for another's benefit with respect to a particular undertaking. A fiduciary must exercise scrupulous good faith and candor to protect the interests of the party or parties served.

Id.

87. *See id.* at 675.

88. A certification practice statement is "a statement of the practices which a certification authority employs in issuing certificates." *See Digital Signature Guidelines*, *supra* note 3, at 32.

> Because a certification authority is in the business of enabling others to rely on its certificates and the digital signatures if its subscribers, the certification authority has a greater duty than an ordinary subscriber to make its certification authority certificate available. A certification authority certificate must be easily and conveniently available for reference in a trustworthy manner.

Id. at 67, cmt. 3.6.1.

89. *See id.* cmt. 1.8.1.

90. *See id.* at 56, cmt. 1.35.5.

> conform. Reference to the widely recognized standards may indicate concisely the suitability of the [c]ertification [a]uthority's practices for another person's purposes, as well as the potential technological capability of the certificates issued by the [c]ertification [a]uthority with repositories and other systems.[91]

"A certification practice statement is useful in helping subscribers and relying parties distinguish which [c]ertification [a]uthorities provide more reliable representations in the certificates they issue."[92] Thus, the public relies on these certification practice statements when deciding which certification authority to employ. Therefore, in inducing this reliance, a certification authority shall in good faith make candid and accurate representations in the certification practice statement.

ARTICLE B: THE CERTIFICATION AUTHORITY SHALL BE A FIDUCIARY TO HIS SUBSCRIBER AND RELYING THIRD PARTIES.

Certification Authorities also serve as "limited purpose agents of document signers, and become fiduciaries of those signers, at least as to certain of the fiducial obligations."[93] "A certification authority is a fiduciary to a subscriber where a certification authority holds the subscriber's private key or where provided by contract."[94] A certification authority is a fiduciary to a subscriber and also any relying party[95] where provided by contract or by law.

A certification authority issues a certificate whereby the certification authority notifies the subscriber listed in the certificate of the contents of the certificate. The certificate lists "a [c]ertification [a]uthority as a subscriber and contains a public key corresponding to a private key used to digitally sign another certificate."[96] When issuing such a certificate the certification authority makes certain representations that may induce reliance. The certification authority's representation regarding issuance and acceptance of a certificate provides that the certification authority represents to persons who rely on the certificate that the certification authority has issued a valid certificate.[97] If the certification authority

---

91. *See id.* at 33, cmt. 1.8.4.

92. *See id.* at 33, cmt. 1.8.1.

93. *See* Closen, *supra* note 4, at 675. *See also* Survey, *supra* note 27, (stating in response to question (3) 60 percent of those surveyed believed that a Certification Authorities are fiduciaries to their clients).

94. *See Digital Signature Guidelines*, *supra* note 3, at 62, cmt. 2.4.

95. A relying party is "a person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them." *Id.* at 48, cmt. 1.27. The relying party relies upon the certificate to bind the public key to the identity of the subscriber.

96. *See id.* at 32, cmt. 1.7.

97. *Id.* at 68, cmt. 3.7.

> By issuing a certificate, a Certification Authority represents to any person who reasonably relies on a certificate or a digital signature verifiable by the public key listed in the certificate, that the Certification Authority, in accordance with any

has also published the certificate, the certification authority also represents that the subscriber has accepted the certificate and that the certificate is valid. A certification authority must not publish and/or disclose a certificate known to be unaccepted by the subscriber.[98] Disclosure of such a certificate will make that certificate invalid. "If a certificate is not valid, a relying party will not be able to use it to verify the digital signature of a subscriber, and thus will have diminished ability to enforce the subscriber's digital signature against the subscriber."[99]

When a certification authority issues a certificate it is foreseeable that the parties will rely on the certification authority's representations. The reliance that a certificate creates is two-fold. First, the relying party relies upon the verification of the digital signature to provide assurance that the private key corresponding to the public key listed in the certificate was used by the signer. Second, the relying party relies upon the accuracy of the certification authority's representations in the certificate, particularly the assurance that the signer who holds the private key corresponding to the public key listed in the certificate is in fact the subscriber identified in the certificate, and not an impostor.[100] Thus, the certification authority shall make accurate and truthful representations.

A certification authority has a fiducial relationship to the relying parties not to make inaccurate or dishonest misrepresentations in the certificate. This fiduciary relationship exists where the certification authority holds the private key of a subscriber or by agreement such as a subscriber agreement or a certification practice statement.[101]

The certification authority who provides ancillary services shall also be a fiduciary to his or her client. Certain ancillary services may demand

---

applicable certification practice statement of which the relying person has notice, has confirmed that: (1) the certification authority has complied with all applicable requirements of the signature guidelines in issuing a certificate, and if the certification authority has published the certificate or otherwise made it available to such reasonably relying person, that the subscriber listed in the certificate has accepted it, (2) the subscriber identified in the certificate holds the private key corresponding to the public key is listed in the certificate, (3) if the subscriber is acting through agents, that the agents have the authority to accept the certificate for the subscriber, (4) the subscriber's public key and private key constitute a functioning key pair, and (5) all information in the certificate is accurate, unless the certification authority has stated in the certificate or incorporated by reference in the certificate that the accuracy if specified information is not confirmed. Further, the certification authority represents that there are no known, material facts omitted from the certificate which would, if known, adversely affect the reliability of its representations under the digital signature guidelines.

Id.

98. *See Digital Signature Guidelines*, *supra* note 3, at 41, cmt. 1.16.6.

99. *See id.* at 41, cmt. 1.16.5.

100. *See id.* at 62, cmt. 2.3.1.

101. *See id.* at 62, cmt. 2.4.2.

"fiduciary-like" certification services.[102] The certification authority should also have the responsibility of "advising the entruster of relevant information that comes to the attention of the fiduciary in the course of fiducial activities."[103] "Fiduciaries should fully and accurately advise their entrusters on matters within the professional expertise of the fiduciaries," and that includes the attorney certification authority.

V. GUIDING PRINCIPLE IV

A. The Certification Authority Owes a Standard of Care to Their Clients

IV-A: THE CERTIFICATION AUTHORITY SHALL CONFIRM FACTS TRANSACTIONALLY RELATED TO ISSUING A CERTIFICATE.

Directive:

The certification authority has a duty to investigate facts supporting a certificate issuance.

IV-B: THE CERTIFICATION AUTHORITY SHALL SAFEGUARD PRIVATE KEYS.

Directive:

The certification authority shall secure personal and sensitive information contained in private keys. The certification authority shall guard against compromising a private key.

IV-C: THE CERTIFICATION AUTHORITY SHALL MAINTAIN PROPER RECORDS.

Directive:

The certification authority shall maintain an electronic record of each cybernotary transaction. This electronic record is the certification authority's journal.

IV-D: THE CERTIFICATION AUTHORITY SHALL MAINTAIN CONFIDENCES THAT ARE TRANSACTIONALLY RELATED TO HIS CYBERNOTARY FUNCTIONS.

Directive:

The certification authority shall protect the confidences of electronic document signers and notarized documents.[104]

IV-E: THE CERTIFICATION AUTHORITY SHALL DISCLOSE FACTS THAT ADVERSELY OR MATERIALLY AFFECT RELIANCE.

Directive:

---

102. *See id.* at 62, cmt. 2.4.3.

103. *See* Closen, *supra* note 4, at 671.

104. Just like attorneys, Certification Authorities should maintain client confidences. *See* Model Code of Professional Responsibility Canon 4 (1980).

A certification authority shall disclose any known fact adversely and materially affecting reliance upon a certificate or a digital signature verifiable by reference to a public key listed in a certificate.[105]

IV-F: THE CERTIFICATION AUTHORITY SHALL AVOID CONFLICTS.

Directive:

A certification authority shall refrain from issuing a certificate, if doing so; he or she would receive any advantage or benefit, including non-financial ones, from the transaction.[106]

IV-G: THE CERTIFICATION AUTHORITY SHALL HAVE SUFFICIENT FINANCIAL RESOURCES.

Directive:

A certification authority shall have sufficient financial resources to bear his or her risk of liability to subscribers and relying third parties.

B. COMMENTARY—GUIDING PRINCIPLE IV

General Comments:

The certification authority is an attorney with a highly skilled technical background. Thus the standard of care a certification authority owes to his or her client is a professional standard of care.

ARTICLE A: THE CERTIFICATION AUTHORITY SHALL CONFIRM FACTS TRANSACTIONALLY RELATED TO ISSUING A CERTIFICATE.

A certification authority has a duty to investigate the facts supporting a certificate issuance. The certification authority shall ascertain through appropriate inquiry and investigation whether the representations he or she makes in a certificate are accurate and truthful.[107]

In determining what level of inquiry and investigation is appropriate, a certification authority may consider "the probable use of a certificate based on the prospective subscriber's representations, the prospect of reliance on the certificate, and any effective limits on reliance."[108]

When confirming facts that are transactionally related to the issuance of a certificate, the certification authority is not obligated to guarantee or underwrite the factual accuracy of the confirmed information.

> The level of investigation required [for confirming facts] will vary according to the circumstances for which a certificate is intended, and may be increased by a certification practice statement or contract. The [c]ertification [a]uthority may specify in a certification practice state-

105. *See Digital Signature Guidelines*, *supra* note 3, at 64, cmt. 3.2.2.

106. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 13.

107. *See* DIGITAL SIGNATURE GUIDELINES, *supra* note 3, at 34, cmts. 1.9, 1.9.1. *See also* MODEL RULES OF PROFESSIONAL CONDUCT Rule 4.1 (1983) (stating an attorney must not make false statements of law or fact).

108. *See Digital Signature Guidelines*, *supra* note 3, at 34, cmt. 1.9.2.

ment the detailed methods and practices for confirming the information in the certificate.[109]

ARTICLE B: THE CERTIFICATION AUTHORITY SHALL SAFEGUARD PRIVATE KEYS.

The certification authority shall secure both private and public keys.[110] Encryption technology plays a critical role in the certification authority's ability to safeguard information contained in private keys.[111] Thus the certification authority must implement trust systems as a way to safeguard sensitive information and facilitate trust and confidence in the electronic stream of commerce.

The certification authority shall not disclose or compromise any information relating to a private key. Normally, the subscriber holds a private key.[112] The subscriber creates the private key or has been provided it for his or her use, and the subscriber has the responsibility not to compromise the private key corresponding to a public key listed in the certification authority's certificate.[113] However, there are circumstances where the certification authority has access to a private key. Such circumstances include specialized organizational considerations or other ancillary services such as a commercial key escrow service or a private key trust service. When a certification authority has access to the information stored in a private key, the certification authority has a duty to safeguard the private key.

If the private key is compromised, and a certification authority has already issued a certificate listing the corresponding public key, then the certification authority shall take appropriate corrective action by either revoking the certificate or suspending the certificate without delay until revocation can be effected.[114] The Subscriber may, but does not have to, initiate the suspension or revocation by requesting the issuing certifica-

109. *See id.* at 34, cmt. 1.9.3.

110. *See* Ahlers, *supra* note 31, at 919 (stating that Cybernotaries are going to safeguard public and private keys).

111. UTAH CODE ANN. §§ 46-3-103 to 46-3-309 (West 1996).

> A certification authority's overall risk of liability will largely be a function of [1] its successes in implementing a trustworthy system and utilizing the services of competent, conscientious personnel, [2] the number of certificates outstanding, and [3] the amounts at stake in transactions in which issued certificates are used, all evaluated in light if any applicable limits upon legal liability and cautionary notices of recommended reliance limits. The certification authority can control factors [1] and [2], bur can do little to manage the risk in regard to factor [3], unless an applicable certification practice statement or legislation states that issued certificate is not suitable for transactions in excess of monetary amount specified either generally in the certificate practice statement or specifically in regard to a particular certificate.

Id.

112. *See Digital Signature Guidelines*, *supra* note 3, at 37, cmt. 1.14.1.

113. *See id.* at 80, cmt. 4.3.

114. *See id.* at 80, cmt. 4.3.5.

tion authority to suspend or revoke the certificate.[115]

ARTICLE C: THE CERTIFICATION AUTHORITY SHALL MAINTAIN PROPER RECORDS.

> Maintaining proper records includes the maintenance of a journal. Such a record would be electronic and permanent, documenting the cybernotary's conduct in every electronic transaction. The record would have to be secure, tamper-proof and available for public review to verify a notarial act or to resolve a disputed transaction. The journal record must show that every electronic notarial act is documented chronologically and that the requisite prerequisites for correct and diligent cybernotarizations are followed.[116]

The record should also include time, and essential details involved in the cybernotarization process.[117]

The certification authority shall document all facts material to the issuance, suspension or revocation of a certificate.[118] Records documenting the issuance of a particular certificate may include methods evidencing steps to confirm the identity of the subscriber and other facts represented by the certification authority in issuing a certificate.[119]

The certification authority shall maintain this record for an appropriate period of time—depending on the type of transaction involved. The record retention period may depend on various factors, including but not limited to, contractual obligations to subscribers, statutory record retention requirement, and business needs.[120]

Maintenance of an electronic journal is beneficial. First, an electronic record will help protect a certification authority against allegations of misconduct.[121] Second, an electronic journal serves the public interest because a record will help trace any fraudulent transaction. Moreover, such a record will help deter fraud by requiring the certifica-

---

115. *See id.* at 81, cmt. 4.4.

116. *See* Peter J. Van Alstyne, *The Notary's Duty To Meticulously Maintain A Notary Journal*, 31 J. MARSHALL L. R. 777, 800 (1998); NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 32.

117. *Final Report of the Comm. on Elec. Commerce and Crime*, *supra* note 39 at 35, cmt. 8.

> A secure signature must be both created and linked to an electronic record being signed in a manner such that if either the record or the signature is altered after the signature is made, the fact of such alteration is disclosed to persons relying on the electronic record. This is a key requirement for a secure signature, as otherwise the electronic signature of one person could be altered to look like the electronic signature of another, or an electronic signature could be simply excised from one electronic record and pasted onto another.

Id.

118. *See Digital Signature Guidelines*, *supra* note 3, at 66, cmt. 3.5.

119. *See id.* at 66, cmt. 3.5.1.

120. *See id.* at 66, cmt. 3.5.3.

121. *See* Van Alstyne, *supra* note 103, at 800.

tion authority to obtain important information incident to the cybernotarization that impostors may not be able to produce.[122]

ARTICLE D: THE CERTIFICATION AUTHORITY SHALL MAINTAIN CONFIDENCES THAT ARE TRANSACTIONALLY RELATED TO HIS CYBERNOTARY FUNCTIONS.

The Certification Authority shall respect the privacy of an electronic document signer and not divulge personal or proprietary information disclosed during the execution of a cybernotarial act.[123] Failure to observe confidences is unprofessional and constitutes a breach of public trust.[124]

As an attorney, the Certification Authority is bound by the Attorney code of professional responsibility to maintain client confidences.[125]

ARTICLE E: THE CERTIFICATION AUTHORITY SHALL DISCLOSE FACTS THAT ADVERSELY OR MATERIALLY AFFECT RELIANCE.

> [The] [c]ertification [a]uthority must disclose any material certification practice statement, as well as notice of the revocation or suspension of a certificate authority certificate. A certification authority must also use reasonable efforts to notify any persons who are known to be or foreseeably will be affected by the revocation or suspension of a certificate.[126]
>
> In the event of an occurrence which materially and adversely affects a [c]ertification [a]uthority's trustworthy system or his certificate, the [c]ertification [a]uthority must use reasonable efforts to notify any persons who are known to be or foreseeably will be affected by that occurrence, or act in accordance with procedures specified in his certification practice statement.[127]

A certification authority may choose to disclose further information in order to reduce his or her risk of liability.

ARTICLE F: THE CERTIFICATION AUTHORITY SHALL AVOID CONFLICTS.

The certification authority shall conduct cybernotarizations without receiving any improper personal gains or profits [other than the fee charged]. Receiving such improper gains creates the appearance of impropriety and perceived conflicts of interests as well as a breach of ethical conduct.[128] "Ethical concerns dictate a ([c]ertification [a]uthority) take all reasonable steps to avoid a conflict of interest, notwithstanding the fact that an action at issue may otherwise be legal."[129] The presumption is that the conflict of interest may motivate the certification

122. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 33.
123. *See* Closen, *supra* note 4, at 667.
124. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 37.
125. *See* MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1983).
126. *See Digital Signature Guidelines*, *supra* note 3, at 63, cmt. 3.2.
127. *Id.*
128. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 13.
129. *Id.*

authority to issue a certificate for the sake of personal gain instead of following proper cybernotary procedures.

Because certification authorities are attorneys, the problems associated with conflicts of interest become more acute.[130] At issue is whether the attorney certification authority's financial incentive will result in a cybernotarization that does not serve the client and those who rely in the cybernotarization itself. Impartiality is compromised when a certification authority has a personal interest in the issued certificate or the transaction to be cybernotarized.

ARTICLE G: THE CERTIFICATION AUTHORITY SHALL HAVE SUFFICIENT FINANCIAL RESOURCES.

> A certification authority shall have sufficient financial resources to maintain his or her operations in conformity with his or her duties, and to be reasonably able to bear his or her risk of liability to subscribers and relying parties on certificates issued by him or her and digital signatures verifiable by reference to public keys listed in such certificates.[131] Financial resources may take the form of security arrangements like surety bonds, standby letters of credit, or even liability insurance.[132]

VI. GUIDING PRINCIPLE V

A. THE CERTIFICATION AUTHORITY HAS A DUTY TO GUARD AGAINST FRAUD AND PROMOTE TRUTHFULNESS IN TRANSACTIONS

V-A: THE CERTIFICATION AUTHORITY SHALL PASS A CRIMINAL BACKGROUND CHECK.

Directive:

A certification authority cannot issue certificates or be entrusted with private and public keys unless he or she first passes a criminal background check. If someone has been convicted of fraud, that person should not become a certification authority.

V-B: THE CERTIFICATION AUTHORITY MUST PROCURE PROPER IDENTIFICATION.

Directive:

The certification authority must procure proper identification of relevant parties before issuing a certificate. The certification authority shall record these identifications in an electronic journal.

V-C: THE CERTIFICATION AUTHORITY SHALL VERIFY INFORMATION.

Directive:

---

130. *Id.*

131. *See Digital Signature Guidelines*, *supra* note 3, at 64, cmt. 3.3.

132. *See id.* at 65, cmt. 3.3.3.

The certification authority shall verify and confirm information before issuing a certificate.

V-D: THE CERTIFICATION AUTHORITY SHALL TIME STAMP CERTIFICATES.

Directive:

The certification authority shall include in a certificate the correct date and time of an action and the identity of the person that created the notation.[133]

V-E: THE CERTIFICATION AUTHORITY SHALL SUSPEND OR REVOKE A CERTIFICATE WHEN A PRIVATE KEY IS COMPROMISED.

Directive:

If an entrusted party loses control of a private key, the private key is compromised and the certificate becomes unreliable. When this happens, the certification authority shall suspend or revoke an unreliable certificate. Immediately thereafter, the certification authority must publish notice of the revocation or suspension.[134]

V-F: THE CERTIFICATION AUTHORITY SHALL REPORT FRAUDULENT ACTIVITY.

Directive:

The certification authority shall report to appropriate law enforcement or disciplinary authorities any illegality requested, required, proposed or performed that involves a cybernotarial act or issuance of a certificate by that certification authority or by any other certification authority.[135]

B. COMMENTARY—GUIDING PRINCIPLE V

General Comments:

Electronic document certification is a nonrepudiation service. "A nonrepudiation service provides evidence to prevent a person from unilaterally modifying or terminating legal obligations arising out of a transaction effected by computer-based means."[136] Signer authentication and document authentication are essential components of this service because they exclude impersonators and forgers.[137] Certification authorities affix digital signatures on certificates thereby providing the greatest possible assurance of both signer authenticity and document authenticity. Thus, certification authorities play a role in this nonrepudia-

133. *See id.* at 52.

134. *See id.* at 16.

135. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 23, IV-E-3.

136. *See Digital Signature Guidelines*, *supra* note 3, at 7.

137. *Id.*

tion service.[138]

A paramount function of a certification authority is to guard against fraud. A certification authority can guard against fraud by verifying and confirming facts and by procuring proper identification of relevant parties. Furthermore, a certification authority should time stamp each transaction and keep an electronic record of all transactions. Another way a certification authority can guard against fraud is by preventing unauthorized use of his or her digital signature device[139] and to report any fraudulent activities.

A certification authority can promote truthfulness in cybernotary transactions by issuing only reliable certificates and suspending or revoking the unreliable certificates.

ARTICLE A: THE CERTIFICATION AUTHORITY SHALL PASS A CRIMINAL BACKGROUND CHECK.

A certification authority is in a unique position because not only is he or she entrusted with sensitive data and verifies signer and document authenticity, the certification authority, as an attorney, also performs important ancillary services. Thus, an unscrupulous certification authority has access to the kind of information that can easily be exploited for personal gain or to commit fraud. Hence, it is of vital importance that a certification authority passes a criminal background check because one who has a proclivity or a history in engaging in fraudulent activities should not be allowed to hold the office of a certification authority.

ARTICLE B: THE CERTIFICATION AUTHORITY MUST PROCURE PROPER IDENTIFICATION.

In an effort to prevent fraud, the certification authority should collect several forms of identification of the relevant parties engaged in a transaction. Proper identification may include, but is not limited to, the following requirements. First, the certification authority should obtain a photo identification of the parties the certification authority certifies in a transaction. For example, a certification authority may request to see a party's driver's license. Second, the certification authority should obtain a digital thumbprint[140] of the parties involved in the transaction.[141]

> To obtain a finger image, one places the finger or thumb on a template attached to a computer, which scans a reproduction of the print into the

138. *See id.* at 6-11.

139. *See* 15 ILL. COMP. STAT. 335/14; 625 ILL. COMP. STAT. 5/6 (West 1998).

140. A fingerprint is an impression formed by the underside of every human finger and is useful for identification purposes because no two people possess exactly the same print. 4 ENCYCLOPEDIA BRITANNICA *Fingerprint* 781 (15th ed. 1992).

141. For a general discussion as to why a biological identifier, like a thumbprint, should be used in notarized transactions, see generally Vincent J. Gnoffo, *Requiring a Thumbprint for Notarized Transactions: The Battle Against Document Fraud*, 31 J. MARSHALL L. REV. 803 (1998).

> computer's memory. Once this is accomplished, one can use the computerized image to distinguish between millions of fingerprints stored in the memory.[142]

The certification authority should record the photo identification and digital thumbprint in an electronic journal. Procuring and recording this identification should become customary practice for the certification authority because this practice can be an effective deterrent against fraud.[143] Because a digital photo and thumbprint is traceable evidence, a party will be more likely to reconsider pursuing a fraudulent activity.

Moreover, a certification authority may rely on the latest technological developments to supplement his or her ways of procuring identification of parties. For instance, the certification authority can conduct a cybernotarial transaction via teleconferencing.[144] The use of video will not only overcome the special problems due to lack of physical presence; this use will also aid the certification authority guard against fraud.[145]

> One way to accomplish this task is to electronically capture the signing of an agreement, digitally signing the video in a manner that shows the parties entering into the transaction, and simultaneously locking the image so that any tampering would be detected . . . the computer could also capture the visual portion of the meeting when the counselors all agreed to the transaction, and digitally wrap the video portion up with the text.[146]

By taking proper precautions like securing the identification of parties and using the latest technological advances in trust systems, the certification authority will play an instrumental role in minimizing or preventing fraud all together. When the chances of fraud go down, confidence in electronic commerce goes up.

ARTICLE C: THE CERTIFICATION AUTHORITY SHALL VERIFY INFORMATION.

A certification authority has a duty to investigate the facts supporting a certificate issuance. The certification authority shall ascertain through appropriate inquiry and investigation whether the representations he or she makes in a certificate are accurate and truthful.[147] The verification or confirmation of facts helps guard against fraud since such

---

142. *Id.* at 812.

143. *Id* at 815 (stating that getting identification aids in prevention of fraud). *See also* NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 18.

144. Teleconferencing is easily accessible to in-home PC users. An individual can choose from having a video phone installed in their PC to a Desktop or Television Set video phone. For information on teleconferencing, see 8x8, Inc., *The Leader in Video Communications* (visited Nov. 18, 1998) <http://www.8x8.com/html>.

145. *See* Faerber, *supra* note 72, at 754.

146. *See* Ahlers, *supra* note 31, at 924.

147. *See Digital Signature Guidelines*, *supra* note 3, at 34, cmts. 1.9, 1.9.1.

an investigation may expose whether a party is intending to engage in a fraudulent activity.

ARTICLE D: THE CERTIFICATION AUTHORITY SHALL TIME STAMP CERTIFICATES.

The certification authority shall time stamp a certificate indicating the correct date and time of an action and the identity of the person that created the notation.[148] A time stamp will help promote truthful transactions because it facilitates proof that the digital signature was created during the operational period[149] of a valid certificate.[150] This proof is critical for the verification process and message integrity of certificates.[151] For example, "a digital signature created after a certificate has expired, been revoked or suspended, or before it has been issued, is not verifiable" and subsequently, invalid. A time stamp on the certification authority's electronic journal may also be useful to prove when a certificate was issued or at least the earliest date and time the certificate could have been issued.[152] This determines the beginning point of the Certificate's operational period.[153]

Additionally, the time and date when the digital signature was created may indicate whether the digital signature is reliable for the purposes of determining whether reliance on such a certificate (with reference to a public key listed in the certificate) was reasonable.[154]

Moreover, time stamping is also important in establishing which version of an extrinsic message is incorporated by reference, and is a useful tool for the performance of many ancillary services.[155]

ARTICLE E: THE CERTIFICATION AUTHORITY SHALL SUSPEND OR REVOKE A CERTIFICATE WHEN A PRIVATE KEY IS COMPROMISED.

If an entrusted party loses control of a private key, the private key is compromised and the certificate becomes unreliable. When this happens, the certification authority (either with or without the subscriber's

148. *See id.* at 52, cmt. 1.33.

149. An operational period is "the operational period of a certificate begins on the date and time it is issued by a certification authority (or on a later date and time certain if stated on the certificate), and ends on the date and time it expires or is earlier revoked or suspended." *Id.* at 45, cmt. 1.22.

150. *See Digital Signature Guidelines*, *supra* note 3, at 30, cmt. 1.5.5.

151. To verify a certificate a certification authority "in relation to a given digital signature, message, and public key, to determine accurately: (1) that the digital signature was created during the operational period of a valid certificate by the private key corresponding to the public key listed in the certificate; and, (2) the massage has nit been altered since its digital signature was created." *Id.* at 58, cmt. 1.37.

152. *See id.* at 30, cmt. 1.5.5.

153. *See id.* at 53, cmt. 1.33.2.

154. *See id.* at 53, cmt. 1.33.3.

155. *See Digital Signature Guidelines*, *supra* note 3, at 52, cmt. 1.33.1.

request[156] depending on the circumstances), shall suspend or revoke an unreliable certificate.[157] Immediately thereafter, the certification authority must publish notice of the revocation or suspension.[158] The certification authority shall also notify persons who inquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate.[159]

ARTICLE F: THE CERTIFICATION AUTHORITY SHALL REPORT FRAUDULENT ACTIVITY.

The certification authority shall report to appropriate law enforcement or disciplinary authorities any illegality requested, required, proposed or performed that involves a cybernotarial act or issuance of a certificate by that certification authority or any other certification authority.[160] As a public official, the certification authority shall neither be a part of nor abet an illegal act. This directive imposes an ethical obligation to report knowledge of cybernotary-related illegalities to the appropriate authority. This obligation is consistent with the certification authority's role as "a fraud-deterrent public official and member of a profession."[161]

VII. GUIDING PRINCIPLE VI

A. THE CERTIFICATION AUTHORITY SHALL REFRAIN FROM CYBERNOTARIZING HIS OWN TRANSACTIONS AND FROM ACCEPTING IMPROPER GAINS

VI-A: THE CERTIFICATION AUTHORITY SHALL REFRAIN FROM CYBERNOTARIZING HIS OWN TRANSACTIONS.[162]

Directive:

---

156. Revocation or suspension without the subscriber's consent:

> A certification authority must suspend or revoke a certificate, regardless if whether the subscriber listed in the certificate consents, if the certification authority confirms that [1] a material fact represented in the certificate is false, [2] a material prerequisite to issuance of the certificate was not satisfied, or [3] the certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability.

See id. at 73-74, cmt. 3.11.

157. *See id.* at 16.

158. *Id.*

159. *Id.*

160. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 23, Article IV-E-3. *See also* MODEL RULES OF PROFESSIONAL CONDUCT Rule 8.3 (requiring attorneys to report any professional misconduct of other attorneys or judges to the ABA disciplinary committee).

161. *Id.* at 24 (stating there is an ethical obligation upon Notaries to deter fraud as a public official).

162. *See* Survey, *supra* note 27, (stating in response to question (5) of those surveyed 80 percent responded that a Certification Authority should not be allowed to notarize their own transactions).

The certification authority shall not cybernotarize his or her own transactions. A subscriber is distinct from a certification authority and the person relying on the subscriber's certificate.[163]

VI-B: THE CERTIFICATION AUTHORITY SHALL NOT EXPLOIT HIS OR HER OFFICE FOR PERSONAL GAIN.

Directive:

The certification authority shall not personally gain from any transaction other than a reasonable fee.

B. COMMENTARY—GUIDING PRINCIPLE VI

ARTICLE A: THE CERTIFICATION AUTHORITY SHALL REFRAIN FROM CYBERNOTARIZING HIS OWN TRANSACTIONS.

The certification authority shall not cybernotarize his or her own transactions. A subscriber is distinct from a certification authority and the person relying on the subscriber's certificate.

Self-cybernotarization creates an appearance of impropriety. Certification authorities, acting in the capacity as attorneys, should not cybernotarize documents they themselves have drafted "because of the appearance of a lack of impartiality and of a financial interest in the documents."[164] This poses a "conflicted practice of lawyers" and should not carry over into international and electronic commerce.[165]

ARTICLE B: THE CERTIFICATION AUTHORITY SHALL NOT EXPLOIT HIS OFFICE FOR PERSONAL GAIN.

The certification authority shall refuse to conduct any transaction that would result, either directly or indirectly, in any actual or potential gain or advantage for the certification authority, financial or otherwise, apart form a fee for issuing a certificate as directed by statue.[166] Furthermore, a certification authority shall not use for personal gain any information extracted from a certificate or other documents that he or she has issued or cybernotarized.[167]

A certification authority is required to disclose any financial interest the certification authority may have in an entity that is a subscriber to that certification authority.[168]

---

163. *See Digital Signature Guidelines*, *supra* note 3, at 51, cmt. 1.31.1.

164. *See* Michael L. Closen, *Reform the Potential Attorney-Notary Conflict*, NAT'L L. J., July 6, 1998, at A24 (stating the National Notary Association, in its Notary Public Code of Professional Responsibility, correctly takes the position that attorney-notaries should not notarize documents they themselves have drafted).

165. *Id.*

166. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 10.

167. *Id.* at 36. It is unethical for an attorney to use client information for personal gain. Hence, a Certification Authority should be held to the same standard. *See* MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.8 (1983).

168. *See Digital Signature Guidelines*, *supra* note 3, at 51, cmt. 1.31.2.

VIII. GUIDING PRINCIPLE VII

A. The Certification Authority Shall Not Purposefully and Knowingly Engage in Misconduct

VII-A: THE CERTIFICATION AUTHORITY SHALL NOT PARTICIPATE IN FRAUDULENT CONDUCT.

Directive:

The certification authority shall not knowingly issue a certificate containing information that is false, deceptive, inaccurate or incomplete.[169] The certification authority shall refuse to perform any cybernotarial act or transaction that is illegal, dishonest, deceptive, fraudulent or otherwise improper.[170]

VII-B: THE CERTIFICATION AUTHORITY MAY BE CRIMINALY LIABLE FOR MISCONDUCT.

Directive:

A certification authority may be criminally liable for participating, facilitating or committing an illegal or fraudulent act.

VII-C: THE CERTIFICATION AUTHORITY MAY BE CIVILLY LIABLE FOR NEGLIGENT CONDUCT.

Directive:

A certification authority may be civilly liable to subscribers and relying third parties for negligent conduct.

B. Commentary—Guiding Principle VII

ARTICLE A: The Certification Authority shall not participate in fraudulent conduct.

Certification authority misconduct is defined to include "any action against public interest."[171] Fraudulent activity falls into this category. A certification authority shall not knowingly issue fraudulent certificates or perform fraudulent cybernotarizations or other activities transactionally related to the profession. The certification authority shall refuse to perform any notarial act in connection with a document or transaction that the [certification authority] knows, or has reason to know, is illegal, dishonest, deceptive, false or improper.[172] Furthermore, the certification authority shall report any such illegality or fraudulent activity to the proper authorities.

---

169. Notary Public Code of Professional Responsibility, *supra* note 11, at 21, IV-B-1 (stating that a Notary shall not knowingly issue certificates containing false information).

170. *Id.* at 22, IV-E-1 (stating that a Notary shall not perform any fraudulent notarization or transaction).

171. *Id.* at 14 (citing Conn. Gen. Stat. § 3-94a(7)(B) (West 1998) for the definition of Notary misconduct).

172. *Id.* at 22.

By participating in fraudulent, or otherwise illegal conduct, the certification authority would not only violate public trust, he or she would adversely affect international and electronic commerce. Thus, the stakes are too high for a certification authority to choose to ignore this directive. The certification authority, as a public officer, shall go at great pains to refrain from participating in any illegal activity and go through similar pains to report the same.

ARTICLE B: THE CERTIFICATION AUTHORITY MAY BE CRIMINALLY LIABLE FOR MISCONDUCT.

The certification authority may be criminally liable for participating, facilitating, aiding, abetting or committing an illegal or fraudulent act as required by law.

ARTICLE C: THE CERTIFICATION AUTHORITY MAY BE CIVILLY LIABLE FOR NEGLIGENT CONDUCT.

The relationship between a certification authority and a subscriber is primarily contractual, "whereby a subscriber and certification authority will agree to reinforce and enhance the subscriber's digital signature capability in exchange for a fee or other consideration."[173] Thus, applicable contract law will govern any breach on the certification authority's part.

The relationship between a certification authority and a relying third party may rest upon principles of both contract and tort.[174] "The duties of a certification authority to a third party relying on a certificate are rooted mainly in legal proscriptions against fraud and negligent misrepresentation."[175]

IX. GUIDING PRINCIPLE VIII

A. THE CERTIFICATION AUTHORITY SHALL TREAT ALL PEOPLE EQUALLY

VIII-A: THE CERTIFICATION AUTHORITY SHALL TREAT ALL PEOPLE EQUALLY.

Directive:

The certification authority shall not discriminate in the performance of his official duties on the basis of race, religion, national origin, age, physical disability, gender, or sexual orientation.

COMMENTARY—GUIDING PRINCIPLE VIII

The certification authority must be blind to these distinctions when rendering his or her services. Certification authorities must not refuse

173. *See Digital Signature Guidelines*, *supra* note 3, at 19.

174. *Id.*

175. *Id.*

services to individuals due to the factors listed above.[176] As a public official, the certification authority shall serve all of the public in an "honest, fair, and unbiased manner."[177]

A discriminating certification authority may be liable for violating a party's civil rights.

X. GUIDING PRINCIPLE IX

A. THE CERTIFICATION AUTHORITY SHALL CHARGE REASONABLE FEES

IX-A: THE CERTIFICATION AUTHORITY SHALL CHARGE REASONABLE FEES.

Directive:

The certification authority shall charge only reasonable fees required for each transaction.

B. COMMENTARY—GUIDING PRINCIPLE IX

A certification authority will be required to have knowledge, skill, and expertise to perform services of a legal and technical manner. Therefore, certification authorities shall be compensated accordingly. Factors to be considered as guidelines in determining the reasonableness of a fee should include, but is not limited to, the following: the time and labor involved; the skill required; the fee customarily charged for a similar service; the nature and length of the client-certification authority relationship; and the experience, reputation and ability of the certification authority performing the service.[178]

A certification authority shall not enter into an agreement for, charge or collect an illegal or clearly excessive fee. A certification authority shall not base the charging or waiving of a fee for performing a transaction, or the amount of the fee, on the person's "race, nationality, ethnicity, citizenship, religion, politics, lifestyle, age, disability, gender or sexual orientation, or on agreement or disagreement with the statements or purpose of a lawful document."[179]

---

176. *See* Closen, *supra* note 4, at 686 (stating that Notaries should treat all people equally and not to discriminate in the performance of their official duties). NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 5, I-A-3 (stating that a Notary shall not refuse to notarize a stranger's document due to any prejudice or bias.)

177. *Id.* Not unlike a Judge, a Certification Authority should "avoid bias and prejudice" while performing their duties. *See* MODEL CODE OF JUDICIAL CONDUCT Rule 3B(5)(6) (1990).

178. Not unlike the MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.5 (1983), fees for professional are need easily determined. Similar to attorneys, the cybernotary will need to set fees on a case by case basis.

179. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 5, I-B-1, (stating that it is unethical for a Notary to base or assess a fee due to any prejudices or bias).

XI. GUIDING PRINCIPLE X

A. THE CERTIFICATION AUTHORITY HAS A DUTY TO MAINTAIN THE INTEGRITY OF THE PROFESSION

X-A: THE CERTIFICATION AUTHORITY SHALL MAINTAIN THE INTEGRITY OF THE PROFESSION.

Directive:

The certification authority shall conduct himself or herself with the dignity befitting a public officer and in a manner that does not bring disrepute or discredit upon the cybernotarial office.

X-B: THE CERTIFICATION AUTHORITY SHALL REPORT MISCONDUCT.

Directive:

The certification authority shall report their colleagues' misconduct.

X-C: THE CERTIFICATION AUTHORITY SHALL MAKE DIGNIFIED ADVERTISEMENTS.

Directive:

The certification authority shall not advertise their services in an excessively commercial manner. The certification authority shall not misrepresent his or her office or make false claims about his or her power, authority, advantages or rights that the office does not give, or use generally misleading language.

X-D: THE CERTIFICATION AUTHORITY SHALL REFRAIN FROM MAKING ENDORSEMENTS.

Directive:

The certification authority shall not use his or her office "to endorse, extol, denigrate a product, service, program, proposal, individual, candidate, organization or contest, or to corroborate or disprove claims about them."[180]

B. COMMENTARY—GUIDING PRINCIPLE X

ARTICLE A: THE CERTIFICATION AUTHORITY SHALL MAINTAIN THE INTEGRITY OF THE PROFESSION.

Certification authorities must perform in a businesslike manner, basing their actions on proven practices of business and government, and carefully document their official activities.[181]

---

180. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 6, I-D-3 (stating it is unethical for a Notary to use the Notary's seal in an improper endorsement). *See also* MODEL CODE OF JUDICIAL CONDUCT Rule 2B (1990) (stating "[a] Judge shall not lend the prestige of judicial office to advance the private interests of the judge or others").

181. Both attorneys and judges are required to maintain the integrity of the legal system. Accordingly, the Certification Authority should maintain the integrity of their profes-

ARTICLE B: THE CERTIFICATION AUTHORITY SHALL REPORT MISCONDUCT.

A certification authority may maintain professional standards by reporting misconduct. The certification authority shall report statutory violations, regulations, and directives governing the conduct of certification authorities.[182] The only way for a profession to earn its deserved recognition is for its members to enforce fair and reasonable standards. Regrettably, it is not enough for a member to learn and abide by the standards, he or she must be willing to protect the integrity of the group by reporting violations when discovered. Only by honest self-policing can [certification authorities] elevate themselves to the status of professionals.[183]

ARTICLE C: THE CERTIFICATION AUTHORITY SHALL MAKE DIGNIFIED ADVERTISEMENTS.

Another aspect of professional behavior includes making dignified advertisements and refraining from making endorsements. A certification authority shall respect his or her office by refraining from advertising his or her services in an undignified and excessively commercial manner. Furthermore, the certification authority shall refrain from making misleading or false advertisements about the cybernotarial office.[184] The misrepresentation of the cybernotarial office is a serious breach of one's professional obligation, and in some instances, may violate the law.

ARTICLE D: THE CERTIFICATION AUTHORITY SHALL REFRAIN FROM MAKING ENDORSEMENTS.

The certification authority shall refrain from using his or her title for making endorsements of a product, service, program, proposal, individual, candidate, organization or contest, or to corroborate or disprove claims about them. Endorsements are an improper use of a certification

---

sion. *See* MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 1 (1980); MODEL CODE OF JUDICIAL CONDUCT Canon 1 (1990).

182. Like the legal profession, Certification Authorities need to self govern their profession. *See* MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 8 (1980) (stating part of a lawyer's duty to improve the legal system, a lawyer should report and testify about violations). *See also* NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 39, X-C-1 (stating a Notary has a duty to report misconduct by other Notaries).

183. *See* NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 40, Article C.

184. Attorneys have many restrictions on the way they can advertise and solicit business. One of the major thrusts of attorney advertising is that is cannot be false or misleading, make unjustified expectation, make unverifiable comparisons, or imply results by improper means. *See* MODEL RULES OF PROFESSIONAL CONDUCT Rules 7.1, 7.2 (1983).

authority's office.[185]

XII. CONCLUSION

Ethical considerations penetrate every aspect of notarization in cyberspace. The proposed code of professional responsibility was drafted to serve several different purposes. They are intended to protect Internet consumers from unscrupulous and incompetent cybernotaries as well as protect Internet consumers from fraud that may arise from cybernotarial conduct. The proposed code is also intended to protect the integrity of authenticating and verifying paperless transactions. Finally, they are intended to regulate the client-cybernotary relationship and define what the practice of notarization really is. No person is really a cybernotary until they have clients for whom they do work. Within this relationship, the proposed code of professional responsibility attempts to protect clients from unauthorized disclosure or confidential information and to assure the integrity of the transactions. As a fiduciary, the cybernotary needs to be a more sophisticated group of individuals to carry out the duties of their public office and insure the trust and confidence of the Internet consumers and international businesses they serve.

185. NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY, *supra* note 11, at 10, Article D (stating it is improper for Notaries to make endorsements) (citing UTAH CODE ANN. § 46-1-10 (West 1996) and WASH. ADMIN. CODE § 308-30-160 (West 1998)).

APPENDIX

GUIDING PRINCIPLES

THE CERTIFICATION AUTHORITY IS A LICENSED ATTORNEY WHO HAS THE DUTY TO BE COMPETENT

THE CERTIFICATION AUTHORITY HAS INTERNATIONAL JURISDICTION

THE CERTIFICATION AUTHORITY SHALL BE A FIDUCIARY

THE CERTIFICATION AUTHORITY OWES A STANDARD OF CARE TO THEIR CLIENTS

THE CERTIFICATION AUTHORITY HAS A DUTY TO GUARD AGAINST FRAUD AND PROMOTE TRUTHFULNESS IN TRANSACTIONS

THE CERTIFICATION AUTHORITY SHALL REFRAIN FROM CYBERNOTARIZING HIS OR HER OWN TRANSACTIONS AND FROM ACCEPTING IMPROPER GAINS

THE CERTIFICATION AUTHORITY SHALL NOT PURPOSEFULLY AND KNOWINGLY ENGAGE IN MISCONDUCT

THE CERTIFICATION AUTHORITY SHALL TREAT ALL PEOPLE EQUALLY

THE CERTIFICATION AUTHORITY SHALL CHARGE REASONABLE FEES

THE CERTIFICATION AUTHORITY HAS A DUTY TO MAINTAIN THE INTEGRITY OF THE PROFESSION