Global Business & Development Law Journal

Volume 15
Issue 2 *Symposium: Beyond Napster -- The Future of the Digital Commons*

Article 14

1-1-2002

I Accept, But Do They? ... The Need for Electronic Signature Legislation on Mainland China

Ian A. Rambarran
University of the Pacific, McGeorge School of Law

I Accept, But Do They? . . . The Need for Electronic Signature Legislation on Mainland China

Ian A. Rambarran[*]

TABLE OF CONTENTS

---

* J.D., University of the Pacific, McGeorge School of Law, to be conferred July 2003; B.A. International Relations, Florida International University, May 1998. This Comment is dedicated to my parents, Harry and Edna Rambarran. Thanks to my well understanding fiancée Beatriz Perez, my awesome editors, Darin, Kelly, Leslie, and Tonya, and to my advisor, Faye Jones.

I. INTRODUCTION

Growth projections for business conducted over the Internet are outstanding.[1] By 2003, global e-commerce[2] sales are forecasted to reach $70 billion.[3] This growth is partially attributed to small businesses beginning to act like multinationals[4] by penetrating international markets, and partially because of multinationals implementing their global strategies.[5] These changes in business strategy necessitate a change in the manner in which business is conducted. Handshakes and ink signatures are steadily being replaced by the click of a mouse or an electronic signature.[6] With China's entry into the World Trade Organization,[7] businesses will seek to utilize these new methods to penetrate the Chinese Internet market. As businesses take advantage of the new opportunities within China, the forecasts for global e-commerce will rise.[8]

Although China has enacted legislation addressing some aspects of e-commerce transactions, it has not taken the same definitive steps regarding the

---

1. *See* Reno v. A.C.L.U., 521 U.S. 844, 851 (1997) for a complete discussion on the Internet and its origins.

2. The term 'e-commerce' means "the use of the Internet for business-to-business and business-to-consumer transactions." WEBSTER'S NEW WORLD DICTIONARY OF COMPUTER TERMS 182 (8th ed. 2000) [hereinafter WEBSTER'S].

3. *See* Robert M. Kossick, *The Emerging Disharmony of Electronic Commerce Legislation in Latin America*, 9 TUL. J. INT'L & COMP. L. 387, 393 (2001) (forecasting the explosive growth of e-commerce, particularly when professional services market themselves on the Internet); *see also* Robbie Downing & Ross McKean, *Digital Signatures: Addressing the Legal Issues*, 3 NO. 6 E-COMMERCE L. REP. 9 (stating that business-to-business transactions in the United States will increase some twenty-fold when compared to figures in 2000). In the United States alone, e-commerce between businesses is projected to grow to $6.3 trillion by 2005. *See id.*

4. A multinational corporation is an entity with "operations, subsidiaries, or investments in more than two countries." Dictionary.com, *Multinationals*, *at* http://dictionary.com/search?q=multinationals&r=2 (last visited Feb. 11, 2002) (copy on file with *The Transnational Lawyer*).

5. *See* David Taylor & Felix A. Ortiz, *Encryption-Hindering the Hackers, Some Technical and Legal Issues*, 611 PRAC. L. INST. 743, 745 (2000) (describing the "far-reaching ramifications" the Internet is having on businesses and consumers). For example, businesses are becoming cognizant of the potential promotional value and distribution channel provided by the Internet. *Id.*; *see also* Dan Gebler, *U.S. E-Tailers Still Leery of Global Markets* (Aug. 16, 2000), *available at* http://www.economercetimes.com/perl/printer/4043/ (copy on file with *The Transnational Lawyer*) (reporting that those companies that do not have "a flexible approach to e-globalization may not be competitive in the future").

6. *See infra*, Part II.A for a discussion of electronic signatures.

7. *See* CNN, *China's Long March to WTO Entry* (Dec. 10, 2001), *available at* htpp://www.cnn.com/2001/WORLD/asiapcf/east/09/18/china.wto.timeline/ (copy on file with *The Transnational Lawyer*) (documenting the significant developments "relating to China's 15 year-bid to join the [World Trade Organization]"). China initially applied to join the General Agreement on Tariffs and Trade (GATT) in 1986. *See id.* On October 18, 2000, the Clinton administration gave China "normal trade status with the U.S." *Id.* On November 10, 2001, trade ministers approved China's entry to the World Trade Organization and by December 11, 2001, China became a "fully fledged member of the international trading system." *Id.*

8. *See* Paul D. McKenzie, *Electronic Commerce Law—People's Republic of China*, *at* http://www.perkinscoie.com/resources/ecomm/prc.htm (last visited Sept. 28, 2001) (copy on file with *The Transnational Lawyer*) (noting that there is a large amount of interest in China's e-commerce market because of its potential for growth).

legal status of electronic signatures that many of its trading partners have taken.[9] Legal uncertainty regarding the enforceability of contracts executed with electronic signatures may result. For example, it is unclear whether a contract with a typed name at the end of an e-mail message or a digital signature will have the same binding effect as its ink counterpart.[10] Nevertheless, this area of uncertainty has not been totally ignored. Parts of the Chinese financial industry and the provincial areas have created an infrastructure to support certain electronic signature transactions. In addition, the Chinese national government is currently drafting specific e-commerce legislation.[11]

This Comment focuses upon the measures China must consider before enacting legislation on electronic signatures by comparing and contrasting the steps the United States and the United Nations have already taken. Part II defines the basic concepts behind electronic signatures. Part III highlights the legislative approaches the United States and the United Nations have taken to facilitate e-commerce. Part IV describes the steps China has taken regarding electronic signatures. Part V suggests how China can best approach the issue of electronic signatures and Part VI concludes that China must adopt a legislative scheme regarding electronic signatures in order to maintain a presence in the global e-commerce marketplace.

II. BASIC CONCEPTS IN ELECTRONIC COMMERCE

As businesses rush to take advantage of opportunities over the Internet, they are beginning to use electronic signatures more often to execute agreements. The electronic signature is replacing its ink counterpart and is being used both to show the identity of the signer, as well as to signify assent to the terms of the

---

9. *See* Jiang-Yu Wang, *The Internet and E-Commerce in China: Regulations, Judicial Views and Government Policies,* 18 COMPUTER & INTERNET L. 12, 20 (2001) (surveying various aspects e-commerce legislation in China, including a discussion of domain registration and encryption regulation); *see also* People's Daily Online, *China's Exports Increase to Top 10 Trading Partners, at* http://english.peopledaily.com.cn /20008/16/print2000816_48360.html (last visited Dec. 10, 2001) (copy on file with *The Transnational Lawyer*) (reporting that the United States is China's largest importer, followed by Hong Kong, Japan and the European Union). The United States imported US$28.24 billion worth of goods from China and the European Union imported US$21.33 billion worth of goods. *See id.*

10. *See* Wang, *supra* note 9, at 20; *see also* AMERICAN BAR ASSOCIATION, *Digital Signature Guidelines Tutorial, available at* http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html (last visited Jan. 21, 2001) [hereinafter Guideline Tutorial] (copy on file with *The Transnational Lawyer*) (noting that "[a] signature is not part of the substance of a transaction, but rather of its representation or form"). In general, signatures serve as evidence, ceremony, approval, and give a sense of finality to a transaction. *See id.* Moreover, the signature, at common law, is required in certain transactions to enforce a contract in court. *See id.*

11. *See* Liu Pinxin, *Overview of the High-Level Symposium on China E-commerce Law (Demonstrative Law), at* http://www.civillaw.com.cn/english/Discussions/D1.asp (last visited Sept. 28, 2001) (copy on file with *The Transnational Lawyer*) (highlighting the debate between Chinese lawmakers regarding e-commerce policies); *see also The First Draft of "E-Commerce Law"(Demonstration Law) Finished,* ASIAPORT DAILY NEWS, Aug. 23, 2001, *available for a fee at* http://library.northernlights.com/FB20010823870 000015.html? inid=eS0iOQoehkFyyAX4eA (copy on file with *The Transnational Lawyer*) (reporting that China looked to developed countries while drafting this law).

agreement.[12] This section explores the various types of electronic signatures used in e-commerce and other related basic concepts.

A. *Electronic Signatures*

The phrase "electronic signature" describes a range of techniques used to electronically authenticate[13] a person's identity.[14] For example, a name typed at the end of an e-mail message and an iris scan[15] are both considered forms of electronic signatures.[16] The latter, known as a biometric signature, is created when muscle movements, such as eye movements or handwritten signatures, are caught on "contact sensitive technologies," [17] and transposed to electronically made documents.[18] For example, biometric signature technology records every stroke made by a signer, including the speed with which it was written and the side from which the letter "t" was crossed.[19] While biometric signatures are designed for use at will, they do not immediately verify a person's identity.[20] To verify the authenticity of a biometric signature, it must be submitted for forensic analysis.[21] Only after forensic analysis can a biometric signature be confidently

---

12. *See* Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7031 (2002).

13. Authentication is defined as the "assent to or adoption of a writing as one's own." BLACK'S LAW DICTIONARY 127 (7th ed. 1999).

14. *See* Jane Kaufman Winn, *Couriers Without Luggage: Negotiable Instruments and Digital Signatures*, 49 S.C. L. REV. 739, 740 (1998); *see also* Daniel J. Greenwood & Ray A. Campbell, *Electronic Commerce Legislation: From Written on Paper and Signed in Ink to Electronic Records and Online Authentication*, 53 BUS. LAW. 307, 309 (1997) (noting that electronic signatures can be "magnetic stripe cards with personal identification numbers (PINs), user names and passwords, public-key cryptography, writing tablets with electronic pens and even smart cards that generate a unique access code every few seconds").

15. *See* Jonathon E. Stern, *Business Law ... The Electronic Signatures in Global and National Commerce Act*, 16 BERKELEY TECH. L.J. 391, 396 (2001) (classing an iris scan as a form of biometric authentication that captures an electronic sample of a certain "physiological characteristic"). "Biometric technology can identify an individual through recognition of a fingerprint, signature [and] voice." *Id.* at 395-96.

16. *See id.* at 396; *see also* Greenwood & Campbell, *supra* note 14, at 309 (noting that more sophisticated authentication technologies will be available as technology continues to advance).

17. *See* Marc Gaudreau, *On the Distinction Between Biometric and Digital Signatures, at* http://www.cic.com/enterprise/whitepapers/whitepaper5.asp (last visited Nov. 14, 2001) (copy on file with *The Transnational Lawyer*) (noting that contact sensitive technologies range from personal digital assistants (PDAs) to digitized tablets).

18. *Id.*

19. *See* Communications Intelligence Corporation, *Understanding Electronic Signatures, at* http://www.cic.com/enterprise/whitepapers/whitepaper1.asp (last visited Nov. 14, 2001) (copy on file with *The Transnational Lawyer*) (noting that the stroke dynamics captured by biometric signature are unique to each individual person).

20. *See* California Secretary of State, *Frequently Asked Questions about California's Digital Signature Law and Regulations, available at* http://www.ss.ca.gov/digsig/digsigfaq.htm [hereinafter California FAQs] (last visited Oct. 1, 2001) (copy on file with *The Transnational Lawyer*) (noting that this technology allows for "future verification of the signature"). This is in contrast to other digital signatures discussed herein, because digital signatures are designed to provide instant verification. *See id.*

21. *See* Gaudreau, *supra* note 17 (noting that when the biometric signature needs to be verified, it must go through a forensic analysis similar to that conducted on ink signatures and would entail "expert visual and microscopic examination"). Since biometric technology captures "speed, acceleration, deceleration, and the

attached to a signer.[22]

A "digital signature" is another form of electronic signature. Unlike a biometric signature, a digital signature bears no relation to handwritten signatures.[23] Digital Signature is a term of art referring to an electronic signature created through the public key encryption process.[24] Encryption describes the process of transforming readable text into unintelligible text that cannot be read or interpreted without first being deciphered.[25] The first step in creating a digital signature requires a computer to generate two mathematically interrelated keys;[26] one key remains private and the other is distributed over the Internet to the general public.[27] Next, the private key holder uses the private key to create a digital signature by encrypting an electronic message[28] into unreadable text.[29]

---

amount of time the pen is on and off the paper" it is difficult to imitate. *Id.*

22. *See id.*

23. *See id.* (noting that this type of technology gained its name because it is attributed to a person in the same way an ink signature is); *see also* Stern, *supra* note 15, at 395-96 (highlighting the different types of biometric signatures, and noting that it is not limited to capturing handwritten signatures but may be used to capture other physical characteristics, such as muscle movements of the eye).

24. *See* Andrew B. Berman, *International Divergence: The "Keys" to Signing on the Digital Line -The Cross-Border Recognition of Electronic Contracts and Digital Signatures,* 28 SYRACUSE J. INT'L L. & COM. 125, 128 (2001). A digital signature has also been defined to mean "[a]n encrypted, tamper-proof attestation, usually attached to an encrypted e-mail message or a certificate, that the person or authority signing the certificate is confident that the message's originator is actually the person he claims to be." WEBSTER'S, *supra* note 2, at 162.

25. *See* Berman, *supra* note 24, at 128.

26. A key used in cryptography means "the procedure that is used to encipher the message so that it appears to be just nonsense." WEBSTER'S, *supra* note 2, at 306.

27. The public key is derived from the private key. Telephone Interview with Verisign Technical Support Agent (Mar. 4. 2002). Each time a potential client wishes to contract with a private key owner, a new public key can be generated from the private key and sent to the potential client. *Id.* Alternatively, the public key can be posted on a website, and when a client wishes to contract with the private key holder, the client enters into another encrypted area analogous to a secure telephone line, called a secure socket layer. *Id.* The secure socket layer is the area on the website where a client would enter their personal information, such as banking information, or it could be a login page. *Id.* The potential client knows she is in the secure socket layer when a golden padlock icon appears at the bottom of the active screen. *Id.* In this area, the private key holder and public key user are ensured privacy from outsiders because the secured socket layer is a unique line of communication between the parties. *Id.* Thus, the secret socket layer's unique line of communication allows the same public key to be used simultaneously by multiple users on a website, but forbids each public key user from deciphering communications from other public key users because each user cannot step outside its secure line of communication. *Id.*; *see also* Winn, *supra* note 14, at 762-63 (noting that this process is called asymmetric cryptology and called public key cryptography because two different keys are generated, and it lies in contrast to symmetric encryption (private key) which uses 'single key encryption'); *see also* Downing & McKean, *supra* note 3 (reporting that public key technology was first explained in the 1970s).

28. *See* Greenwood & Campbell, *supra* note 14, at 314 (noting that the electronic message is passed through a hash function that makes a unique "fingerprint" of that message). This hash message is then encrypted with the private key and attached to a plain text message. *Id.* The recipient of the message runs the plain text message through the same hash and compares it to the hash sent from the private key holder. *Id.* In theory, both of these should be identical. *Id.* However, if this message digest has been tampered with, it would generate a completely different message digest. *Id.*

29. *See* Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace,* 34 SAN DIEGO L. REV. 1225, 1228 (1997) (discussing the potential shortcomings of digital signature legislation based on the public key infrastructure model).

Only the public key user engaged in the particular transaction can decipher the message.[30] Thus, "digital signatures are not like... [those]... obtained after signing for a package at UPS."[31] Instead, digital signatures are complex compilations of information made from a sophisticated mathematical formula that can only be deciphered by the key holders.[32]

Digital signatures offer three immediate benefits to users on the Internet. First, a digital signature confirms that the message came from the private key holder because it can only be properly deciphered into readable text by its mathematically related public key.[33] Second, using digital signature technology reveals any alteration of the message.[34] Third, the private key holder cannot deny the origin of the message once it is deciphered with the corresponding public key.[35]

Another commonly used electronic signature is made with symmetric cryptology, or private key cryptography.[36] In contrast to public key cryptography, from which digital signatures are made, private key cryptology is based on the shared private key principle.[37] The most common type of shared secret key is a personal identification number (PIN), like those used at an Automatic Teller Machine.[38] In a shared private key system, each party uses the same key to both encrypt and to decipher a message.[39] This type of electronic signature is already widely used in the electronic financial service network.[40] However, it is generally not utilized by parties without previous contact.[41]

Delivering a shared secret key over the open network can be problematic and costly.[42] For example, sending a PIN via e-mail message is problematic because

---

30. *See id.* at 1228 (highlighting the fact that the underlying technology used to create a digital signature is complex).

31. *See* Berman, *supra* note 24, at 131; *see also* Winn, *supra* note 14, at 741 (noting that these digitized versions of a person's handwriting are also used by retail stores in point of sale transactions).

32. *See* Downing & McKean, *supra* note 3 (describing how to send information to the private key holder with its corresponding public key).

33. *See* Biddle, *supra* note 29, at 1228 (noting that this quality is called "data origin authentication").

34. *See id.* (noting that this benefit is called "message integrity"); *see also* Guideline Tutorial, *supra* note 10 (affirming that "the digital signature also identifies the signed message, typically with far greater certainty and precision than paper signatures. Verification reveals any tampering, since the comparison with the hash result . . . shows whether the message is the same as when signed").

35. *See* Biddle, *supra* note 29, at 1228 (describing this digital signature attribute to be a "non-repudiation" quality); *see also* Guideline Tutorial, *supra* note 10 (emphasizing that a "digital signature cannot be forged, unless the signer loses control of the private key").

36. *See* Berman, *supra* note 24, at 129-30 (noting that the most popular standard of private key encryption is the Data Encryption Standard know as DES).

37. *See* Winn, *supra* note 14, at 760 (reporting that private key technology was first explained in 1977 and was used for sensitive, but not classified, information).

38. *See* Berman, *supra* note 24, at 126.

39. *See id.* at 129-30.

40. *See* Winn, *supra* note 14, at 762 (noting that in 1981, the American Bankers Association adopted the Data Encryption Standard).

41. *Id.* at 763.

42. *See* Berman, *supra* note 24, at 126 (discussing aspects of the a private key encryption based on

third parties can easily intercept the message before it arrives at its final destination.[43] Moreover, physically delivering a secret key is costly, time consuming and inconvenient, especially when parties must travel to make the delivery.[44] Additionally, using a shared secret key requires each party to trust one another to prevent the security of the key from being compromised.[45]

Unlike private key cryptography, when parties use digital signature technology they do not have to resort to the elaborate methods for delivery.[46] The public/private key relationship does not require each party to share a secret key to read and decipher information. Once a key pair is generated, the public key can be distributed over the open network and it will only decipher messages generated with the private key.[47] The mathematical relationship between both keys enables the private key holder to post her public key over the Internet, without ever having to reveal her private key.[48]

B. Certification Authorities

A certification authority "[fills] the need for trusted third party services in electronic commerce by issuing digital certificates that attest to some fact about the subject of the certificate."[49] In other words, certification authorities verify the trustworthiness of the public key and help eliminate misrepresentation. For example, a person with the intent to defraud can distribute a public key and misrepresent that she is a major business. An unsuspecting customer, believing this misrepresentation to be true, may contract with this business by using the corresponding public key. If the customer gives out credit card information or a bank transfer authorization, he will be at a loss when he does not get the item for which he bargained. To avoid this, a certification authority certifies the authenticity of the public key and attributes the key to a person or a business

---

symmetric encryption).

43. *See* Greenwood & Campbell, *supra* note 14, at 308 (noting that this is part of a security risk, inherent in the open architecture of the Internet).

44. *See* Berman, *supra* note 24, at 130.

45. *See* Winn, *supra* note 14, at 763 (offering the remedy of a "central key distribution system" to alleviate the problems associated with the private key distribution).

46. A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 51 (1996) (describing, in detail, the actors within the public key infrastructure and focusing on the role of digital signatures and certification authorities in e-commerce). "Sender and receiver no longer need a secure way to agree on a shared key." *Id.*; *see also* Winn, *supra* note 14, at 763-64 (highlighting the fact that exchanging a public key in a face-to-face transaction is still the most secure way of delivering public keys).

47. *See* Downing & McKean, *supra* note 3, at 2 (explaining that the public key holder can verify the integrity of the message by making a 'hash' of the original text as well to see if the message digest produced is the same as the one sent).

48. *See* Berman, *supra* note 24, at 131 (noting that "most competent implementations of public key encryption never allow the private key to leave the cryptographic token, thus leaving the private key more protected").

49. *See* Froomkin, *supra* note 46, at 55-64 (discussing the significant role that certification authorities play within the public key infrastructure).

entity.[50]

Certification authorities typically attest to the private/public key owner's identity by issuing a digital certificate after verifying that person's identity.[51] Certification authorities verify the owner of a public key by actually supplying the key or by simply researching the identification of the key holder.[52] The digital certificate contains the identity of the certification authority, names or describes an attribute of the subscriber, contains the subscriber's public key, and contains the certification authority's digital signature.[53] Some certification authorities also provide verification of its digital signature via certification by a second certification authority.[54] Ultimately, after the certification authority attests to the ownership of the public key, the potential merchant or customer may feel more confident about conducting e-commerce because the public key can be placed with whomever he or she wishes to deal.[55]

Electronic signatures and certification authorities can close the gap between unfamiliar contracting parties, who may be thousands of miles apart. The relationship between digital signatures and certification authorities builds a viable model to alleviate verification problems. In an effort to legitimize and promote the use of electronic signatures, legislatures around the world have created a wealth of legislation supporting their use.[56]

---

50. *See id.* at 51.

51. *See id.* at 55 (noting that a certification authority could either be a public or private entity, and discussing the role for which the government can build up confidence for business transacting online).

52. *See id.* at 58-59 (noting that some certification authorities offer a hierarchy of certificates that may require people to actually present themselves for verification before a certificate is issued).

53. *See id.* at 57-58.

54. *See* Berman, *supra* note 24, at 132 (describing the concept of having a root certification and noting that some state governments provide the root certification).

55. *See* Kossick, *supra* note 3, at 422 (noting that merchants will engage less in e-commerce if they feel less secure about the "real world identities of the parties with whom they deal"); *see also* Froomkin, *supra* note 46, at 56 (noting that certification authorities do not eliminate all problems and two realistic problems exist that can lead to uncertainty amongst users). First, the certification authority's digital signature on the issued certificate may not be authentic. *See id.* Even when another certification authority certifies the first certification authority's digital signature, questions are still raised regarding the reliability, and the extent to which that certification authority properly researched the identity behind the public key. *See id.* As Michael Froomkin points out, "Certificates-R-Us," a certification authority that makes zero-inquiries may issue a real certificate, but the value of the attestation would be low. *See id.* at 58.

56. For a comprehensive view of legislation on electronic signatures across the world see Chris Kuner & Stewart Baker et al., *An Analysis of International Electronic and Digital Signature Implementation and Initiatives, at* http://ilpf.org/groups/analysis_IEDSII.htm (last modified Sept. 2000) (copy on file with *The Transnational Lawyer*).

III. THE DEVELOPMENT OF ELECTRONIC SIGNATURE LEGISLATION

The genesis of electronic signature legislation can be traced to legislative acts by the United States and the United Nations. [57] The United States addressed legal uncertainties associated with e-commerce transactions by passing the Electronic Signatures in Global and National Commerce Act (E-SIGN).[58] Specifically, E-SIGN validates the use of electronic signatures in the United States, superceding previous laws that required an ink signature.[59] Internationally, the United Nations adopted the Model Law on Electronic Commerce (MLEC)[60] after recognizing both the legislative inadequacies amongst a number of countries and the need for global uniform legislation on e-commerce.[61] Both acts make e-commerce a more reliable and uniform way to conduct business.

A. History of Electronic Signature Legislation

In October 2000, the United States enacted legislation to facilitate the "continued development and improvement of e-commerce and electronic transactions" throughout the country.[62] However, by that time, many states had already enacted their own legislation governing e-commerce and electronic signatures.[63] For example, both Utah[64] and California[65] had previously enacted legislation validating the use of electronic signatures to execute a contract.

---

57. *See* Amilia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reformation*, 72 TUL. L. REV. 1931, 1955 (1998) (reporting that the United Nations' Model Law was the earliest attempt to address e-commerce and that the ABA Model Agreement served as a "foundation" for such a law). The impetus for the Model Law dates back to drafting efforts in 1984. *See id.* at 1947.

58. *See* Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7031(2002); *see generally* Robert A. Wittie & Jane K. Winn, *Electronic Records and Signatures Under the Federal E-SIGN Legislation and the UETA*, 56 BUS. LAW 293 (2000) (providing an in depth discussion of the Electronic Signatures in Global and National Commerce Act).

59. *See* 15 U.S.C. § 7001(a)(2) (establishing that "a contract to [a] transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic records was used in its formation").

60. *See UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, G.A. Res. 51/162, U.N. GAOR, (1996), *available at* http://uncitral.org/english/texts/electcom/ml=ecomm.htm [hereinafter *MLEC*] (copy of file with *The Transnational Lawyer*) (highlighting the goal of better international economic relations).

61. *See id.* at cmt. 3 (noting that some "existing legislation imposes or implies restrictions on the use of modern means of communication").

62. Berman, *supra* note 24, at 144.

63. *See* Boss, *supra* note 57, at 1970 (reasoning that state interest in electronic signature legislation was spawned by "an element of competition to be the center of high-technology commerce").

64. *See* UTAH CODE ANN. §§ 46-3-101-504 (1995). For a discussion on how California's legislation may be preempted by federal legislation see Emilia Currer, Legislative Counsel of California, *Electronic Signatures and National Commerce Act: County Records: 19087* (2001) (copy on file with *The Transnational Lawyer*).

65. *See* CAL. GOV'T CODE § 16.5 (West Supp. 1995).

The legislation enacted by Utah and California illustrates two distinct categories of electronic authentication legislation: one technology-specific[66] and the other technology-neutral.[67] Utah authored technology-specific legislation, dictating that parties exclusively use a certain type of technology, namely digital signatures, when executing a contract.[68] In contrast, California enacted technology-neutral legislation allowing parties to use a wide range of technology in electronic transactions.[69] The adoption of divergent types of legislation modeled after Utah and California has influenced legislative efforts in both the United States and the United Nations.

1. The Utah Digital Signature Act

Utah's efforts to promote e-commerce began with the Utah Digital Signature Act (The Utah Act) in 1995.[70] The Utah Act has served as precedent for technology-specific legislation within the United States and in the international context.[71] The Utah Act[72] is unique in form because it sets a legal standard in which digital signatures may be used and it also defined the role of certification authorities.[73]

The Utah Act was the first piece of legislation to incorporate the use of digital signatures as a means of executing an electronic document.[74] The Utah

---

66. *See* Wittie & Winn, *supra* note 58, at 295 (noting technology-specific legislation mandates only a certain type of electronic signature be used when contracting via electronic means).

67. *See* Boss, *supra* note 57, at 1971 (noting that a technology-neutral law is open ended and allows for different types of electronic authentication).

68. *See* Kuner et al., *supra* note 56 (noting that technology-specific legislation is seen as prescriptive and "allows legislatures and regulatory agencies to play a direct role in setting standards for and influencing the direction of new technologies"); *see also* Boss, *supra* note 57 (recognizing that the Utah Digital Signature Act may be preempted by the Federal Legislation). Nevertheless, the author of this Comment maintains that a discussion of the Utah Digital Signature Act is pertinent because this piece of legislation serves as a model for international technology-specific legislation and offers an alternative form of legislation to that adopted by Congress.

69. *See* Kuner et al., *supra* note 56 (recognizing that this type of legislation is a minimalist approach aimed at facilitating the electronic signature use in general).

70. *See* UTAH CODE ANN. § 46-3-101 (2001).

71. *See* Kuner et al., *supra* note 56.

72. In 2000, Utah enacted a technology-neutral piece of legislation called UETA. *See* UNIFORM ELECTRONIC TRANSACTION ACT § 7(d) (1999), *available at* http://www.lawupenn.edu/bll/ulc/fnact99/1990s/ueta99.htm [hereinafter UETA] (copy on file with *The Transnational Lawyer*); *see also* Ben Bates, *Recent Legislative Development . . . Uniform Electronic Transactions Act*, UTAH L. REV. SOC'Y 935 (2000).

73. *See* Froomkin, *supra* note 46, at 50 (highlighting the fact that "Utah was the first state to attempt to provide a regulatory framework for [certification authorities]"); *see also* Berman, *supra* note 24, at 140 (emphasizing that The Utah Act "provides a legal infrastructure in which users employ repositories, certification authorities, and public key cryptography technology to sign electronic documents in a legally binding fashion").

74. *See* UTAH CODE ANN. § 46-3-403 (defining the requirements that make a digitally signed document as "valid, enforceable, and effective as if it had been written on paper"); *see also* Boss, *supra* note 57, at 1970 (describing Utah as "the home to high-technology companies" dealing with digital signatures); *see also* James A. Johnson, *Enacted State Digital Signature Legislation, at* http://nii.nist.gov/pubs/enstsign/html (last visited

Act made a digitally signed document legally equivalent to a written document when two requirements were met.[75] First, the document had to "bear in its entirety a digital signature."[76] Second, a digital signature was required to be coupled with a digital certificate, issued by a state-licensed certification authority that verified the owner of the public key.[77] Once these requirements were met, a digital signature was equivalent to an ink signature.[78]

The Utah Act sought to regulate certification authorities by offering an incentive of limited liability once certain requirements were met.[79] In order to obtain this safe harbor, certification authorities were required to obtain a license from the Utah Department of Commerce prior to issuing any authentication certificates.[80] Each certification authority was also required to post a guarantee[81] and to meet certain enumerated personnel requirements.[82] For example, licensed certification authorities could not hire persons convicted of a "felony or crime involving fraud, false statements, or deception."[83] If a certification authority met these enumerated requirements, it was immune from liability for any losses created by fraudulent digital signatures.[84] Moreover, any liabilities certification authorities incurred were limited to the amounts specified in the digital certificate.[85]

Oct. 21, 2001) (copy on file with *The Transnational Lawyer*) (describing various state legislation regarding digital signatures); *see also* Berman, *supra* note 24, at 139 (discussing Utah's status as a pioneer regarding digital signatures in the United States).

75. *See* UTAH CODE ANN. § 46-3-403.

76. *Id.* § 46-3-403(1)(a); *see also* § 46-3-103(10) (defining a digital signature as a transformed message "using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether: (a) the transformation was created using the private key that corresponds to the signer's public key; and (b) the message has been altered since the transformation was made").

77. *See id.* § 46-3-403(1)(b)(i)-(ii) (requiring that that the certification authority also have a valid license "at the time the digital signature was created").

78. *See* Boss, *supra* note 57, at 1970 (emphasizing the goal of promoting e-commerce "among parties previously unknown to each other, and to limit liabilities of parties for errors of identification").

79. *See* UTAH CODE ANN. § 46-3-309(2)(a) (noting that if a certification authority does not waive this right, they will only be liable for "any loss caused by reliance on a false or forged digital signature"). Furthermore, a certification authority will not incur liability in excess of the amount specified as in its "reliance limit" when a loss is caused by any factual misrepresentation that should have be confirmed. *Id.* § 46-3-309 (b)(i). Also, a certification authority will not be liable for punitive damages, expectation damages or damages resulting from pain and suffering). *Id.* § 46-3-309(c).

80. *See id.* § 46-3-201; *see also* Johnson, *supra* note 74, at 2 (documenting some of the requirements that a certification authority must fulfill before given the ability to limit liability). Also, noting that obtaining a license is not mandatory. *See id.*

81. *See* UTAH CODE ANN. § 46-3-301(d).

82. *See id.* § 46-3-201(b)-(c); *see also* Berman, *supra* note 24, at 141 (noting that the Utah Act also defines record keeping responsibilities, as well procedures that certification authorities must follow when issuing and revoking certificates).

83. UTAH CODE ANN. § 46-3-201(1)(b).

84. *See id.* § 46-3-309(2)(a).

85. *See* Berman, *supra* note 24, at 141 (explaining the burdens and liability protection that a certification authority will get should it meet the statutory requirements). Certification authorities will be held to a standard of care similar to that of negligence. *Id.*

The Utah Act was the first piece of legislation to give legal effect to digital signatures based on public key cryptography.[86] The primary justification for enacting technology-specific legislation was that digital signatures were presumed to provide "greater security" than other forms of electronic signatures.[87] However, this presumption effectively excluded all other methods of authentication, which may be reliable, in favor of public key cryptography.[88]

Utah is one of several states that enacted technology-specific legislation that gave legal effect to only digital signatures, to the exclusion of other forms of electronic signatures.[89] The Utah Act was prototypical because it was designed to facilitate e-commerce between parties who had no prior relationship.[90] Furthermore, Utah Act created a legal standard, in which digital signatures could be substituted for ink signatures, and it defined the standards in which third parties, such as certification authorities should operate.

2. *California's Digital Signature Legislation*

California's electronic signature legislation evolved in two stages. First, in 1995, California added Section 16.5 to the Government Code.[91] Second, in late 1999, California adopted the Uniform Electronic Transactions Act,[92] with modifications providing for consumer protection.[93] Section 16.5 was particularly influential to the formulation of other bodies of legislation because it was drafted with technology-neutral language.[94]

In 1995, California enacted Government Code Section 16.5, entitled "Digital Signatures."[95] This section only applied to transactions with a government

---

86. *See* Wittie & Winn, *supra* note 58, at 294 (describing the history behind electronic signature legislation).

87. *Id.* at 295 (discussing the fact that digital signature integrity could be compromised if the digital signature software was not "properly incorporated into software applications, operating systems and network").

88. *See* Greenwood & Campbell, *supra* note 14, at 337-38 (adding that some critics claim specific legislation distorts the electronic signature market by "preventing the evolution of the best business practices, technological innovations, and competitive pricing"); *see also MLEC*, *supra* note 60, at cmt. 55 (discussing the unwillingness of international legislatures to tie a law to a specific state of technological development).

89. *See* Wittie & Winn, *supra* note 58, at 296 (highlighting the fact that other states, such as Minnesota, Mississippi, Missouri, New Mexico and Washington have followed Utah by enacting similar technology-specific legislation).

90. *See* Berman, *supra* note 24, at 140-41 (noting that this piece of legislation was structured to give "users confidence [when utilizing] digital signatures as an authentication procedure for [e]-commerce transactions").

91. *See* CAL. GOV'T CODE § 16.5 (West Supp. 1995).

92. *See* CAL. CIV. CODE § 1633.1-1633.17 (West Supp. 2001).

93. *See* Witte & Winn, *supra* note 58, 296; *see also* Alan C. Raul et al., *California Signs Off on Cybercontracts: Legislature Is First to Adopt Uniform Electronic Transactions Act* (Feb. 2000), *at* http://www.sideley.com/cyberlaw/features/california.asp (copy on file with *The Transnational Lawyer*).

94. *See* Boss, *supra* note 57, at 1972-74 (discussing the development of electronic signature legislation and comparing it to the developments on the international level).

95. *See* CAL. GOV'T CODE § 16.5. It should be noted at this point that California's definition of digital signature departs from the customary definition of digital signature, which is considered to be the product of

agency, but nevertheless, gave electronic signatures the same legal effect as ink signatures, provided certain requirements were met.[96] First, the electronic signature had to be uniquely identifiable to the user.[97] Second, the electronic signature needed to be capable of verification.[98] Third, the electronic signature had to be "under the sole control of the person using it."[99] Fourth, the electronic signature needed to be attached to the data in a way that would reveal any changes.[100] Finally, the electronic signature was required to conform to regulations adopted by California's Secretary of State.[101]

Section 16.5 is considered technology-neutral because it allows parties to use multiple forms of electronic signatures to authenticate documents. California defines an electronic signature as "an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature."[102] Allowing such a broad definition permits the use of digital signature alternatives, such as biometric signatures.[103]

The terms of Section 16.5 are deliberately broad because California fears the "over-regulation of an industry that has yet to fully evolve would only serve to stifle the natural market forces that are crucial to the thorough evolution of any emerging technology."[104] California's technology-neutral approach sparked other states to adopt similar legislation.[105] However, Section 16.5 fails to create legal certainty among private parties engaging in e-commerce because it applies to only a narrow class of transactions between the government and private parties.[106]

The rapid growth of opportunities in e-commerce incited many state legislatures to enact legislation regarding electronic signatures. The dilemma each legislature faced was whether to enact a technology-specific piece of legislation or a technology-neutral one. This resulted in divergent law regarding electronic signatures throughout the United States.

---

asymmetric encryption. *See* Webster's, *supra* note 2, at 306; *see also* Berman, *supra* note 26, at 128.

96. *See* California FAQs, *supra* note 20.

97. *See* CAL. GOV'T CODE § 16.5(a)(1).

98. *See id.* § 16.5(a)(2).

99. *Id.* § 16.5(a)(3).

100. *See id.* § 16.5(a)(4).

101. *See id.* § 16.5(a)(5); *see also* Boss, *supra* note 57, at 1972 (discussing legislative efforts in Illinois as echoing the requirements as laid down in California).

102. CAL. GOV'T CODE § 16.5(d).

103. *See* Gaudreau, *supra* note 17; *see also* Communications Intelligence Corporation, *supra* note 19.

104. *See* California FAQs, *supra* note 20.

105. *See* Boss, *supra* note 57, at 1972 (stating that this type of technology-neutral legislation was "more popular in the United States than the Utah focus on digital signatures alone").

106. *See* Johnson, *supra* note 74.

B. The Need for Uniform Legislation

As U.S. states continued to enact conflicting legislation, interstate commerce was burdened by the legal uncertainty regarding the status of electronic signatures.[107] Furthermore, businesses were forced to meet the technology requirements of every state in which they dealt.[108] The Clinton administration noted that a lack of legal certainty dissuaded the public from conducting business on the Internet.[109] With these thoughts in mind, the administration sought assistance in creating a "uniform legal framework that recognizes, facilitates, and enforces electronic transactions worldwide."[110]

1. The Uniform Electronic Transaction Act

Motivated by the lack of uniform state legislation on e-commerce, the National Conference of Commissioners on Uniform State Laws (NCCUSL)[111] sought to accommodate electronic transactions within contract law.[112] The NCCUSL believed that a uniform e-commerce law would promote interstate commerce. [113] Thereafter, the Uniform Electronic Transaction Act (UETA) was proposed to the states.[114] UETA seeks to remove possible legal impediments regarding electronic signatures, without changing the underlying substantive contract law.[115]

UETA affects the medium in which business is conducted by allowing ink signatures to be replaced by electronic signatures.[116] Under Section 7, an electronic signature may not be denied legal effect simply because it is in electronic form.[117] UETA defines an electronic signature as any "sound, symbol or process attached to or logically associated with a record and executed or

---

107. *See* Stern, *supra* note 15, at 391.

108. *See id.*

109. *Id. supra* note 15, at 391 (quoting the Clinton Administration's July 1997 report that encouraged the private sector to address the public's "wariness of conducting extensive business over the Internet because of the lack of a predictable legal environment governing transactions").

110. *Id.*

111. *See* INGEO SYSTEMS, DISCUSSION PAPERS, ELECTRONIC DOCUMENT LEGISLATION 1-2 (2001) [hereinafter DISCUSSION PAPERS] (copy on file with *The Transnational Lawyer*) (describing the NCCUSL to be "an organization of attorneys, judges, and law professors that drafts proposals for uniform legislation and works toward their enactment in state legislatures").

112. *See* Boss, *supra* note 57, at 1963.

113. *See* DISCUSSION PAPERS, *supra* note 111, at 1.

114. *See id.*

115. *See id.* at 2; *see also* Raul et al., *supra* note 93 (noting that UETA is more of a procedural guide than substantive change of the underlying law).

116. *See* UETA, *supra* note 72 (providing that "if a law requires a signature, an electronic signature satisfies the law"). Section 5 does not require parties to the use electronic signatures to make an agreement. *Id.* § 5(a).

117. *Id.* § 7 (noting that the source of this particular section to be the Model Law on Electronic Commerce).

adopted by a person with the intent to sign the record."[118] Similar to California's statute, UETA emphasizes the intent of the parties rather than a single style of electronic signature.[119] Therefore, UETA maintains a technology-neutral approach, leaving the parties to determine both the format and the security measures they wish to utilize.[120]

Although NCCUSL aspired to create uniformity among states through UETA, this goal was not immediately achieved. For example, California was the first to adopt UETA's provisions, but created many exceptions to limit UETA's applicability.[121] Furthermore, California's version of UETA created potential problems because the applicable laws could differ if the contract was formed through both electronic and paper means.[122] Thus, California's modifications thwarted the prospective union of paper and electronic contracts.[123]

However, state support for UETA's technology-neutral provisions has steadily increased. Prior to 2000, twenty-two states enacted a version of UETA,[124] and in the wake of federal legislation, forty-three states have followed suit.[125] Among these states is Utah,[126] reflecting its change from a technology-specific

---

118. *Id.* § 2(8) (noting that the "essential attribute of a signature involves applying a sound, symbol or process with an intent to do a legally significant act"). Further, this section contemplates parties using a digital signature based on asymmetric encryption, it only qualifies as a form of electronic signature and is not the only type that can be used. *Id.* at § 2, cmt. 7; *see also* Boss, *supra* note 57, at 1973 (noting that the drafting committee initially favored the presumption that a "certified digital signature bound the purported signer to the electronic record"). However, these presumptions were eliminated by the time the final draft was finished. *Id.* at 1974.

119. *See* UETA, *supra* note 72, § 2, cmt. 7 (requiring an electronic signature to also be logically associated with the record); *see also* Patricia Fry, *A Preliminary Analysis of Federal and State Electronic Commerce Law, available at* www.uetaonline.com/docs/pfry700.html (last modified July 2000) (copy on file with *The Transnational Lawyer*) (noting that UETA also address issues relating to attribution, where the typical issue under this section is not whether the document is electronically signed, but rather "whose signature appears" on it). UETA allows a party to avoid liability if that party's electronic signature was used when the evidence shows that this party did not intend to create a legally binding obligation. *Id.*

120. *See* DISCUSSION PAPERS, *supra* note 111, at 2 (noting that each party can chose from any technology presently available and also from types available in the near future).

121. *See* Wittie & Winn, *supra* note 58, at 296 (noting that many of the amendments to the NCCSUL approved UETA were spawned by the consumer advocates).

122. *See* Raul et al., *supra* note 93.

123. *See id.*

124. *See* Margot Saunders, *The Dynamics of Consumer Protection In Light of UETA and E-SIGN, at* http:www.consumerlaw.org/e_commerce/dynamics_of_consprotection.html (last visited Nov. 3, 2001) (copy on file with *The Transnational Lawyer*) (listing Arizona, California, Delaware, Florida, Hawaii, Iowa, Idaho, Indiana, Kansas, Kentucky, Maine, Maryland, Minnesota, Nebraska, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Utah and Virginia as all passing a version of UETA).

125. *See* Carol A. Kunze, *What's Happening to UETA in the States, at* http://www.ueatonline.com/hapstate.html (last modified Apr. 6, 2001) (copy on file with *The Transnational Lawyer*).

126. *See* Ben Bates, *Recent Legislative Development . . . Uniform Electronic Transactions Act,* UTAH L. REV. SOC'Y 935 (2000) (discussing various aspects of Utah's version of UETA and noting that "the legislature did not want to 'burden' people with requiring a digital signature if they did not have one"). Senator Lyle Hillyard, the sponsor of the Utah's version of UETA, wanted to preserve party autonomy by allowing them to negotiate what type of electronic signature should be used in their contract. *See id.* Bates also notes that Utah's version of UETA does not interfere with the Utah Act. *See id.*

legislative posture to the technology-neutral approach encompassed in UETA.[127] Furthermore, California may repeal its version of UETA in order to replace it with an approved and recommended version of UETA.[128] Although the goal of uniform law envisioned by the NCCUSL was slowly being achieved, Congress sought a more timely resolution to the issue of divergent legislation.

2. *Electronic Signatures in Global and National Commerce*

By mid-2000, less than half of state legislatures had enacted a version of UETA.[129] The probability of nationwide adoption of UETA was of particular concern to lobbyists from the high technology and financial service industries.[130] Subsequently, these lobbyists asked UETA be used as a model for federal legislation.[131] The Clinton Administration, motivated by the Internet boom, responded and sought to draft a uniform law because the divergent legislation was viewed as the "antithesis of strong and efficient markets."[132]

In June 2000, President Clinton signed E-SIGN into law.[133] E-SIGN was designed to create uniformity among states and to facilitate interstate e-commerce.[134] E-SIGN validates the use of electronic signatures and equalizes them legally with ink signatures, thereby providing legal certainty to parties engaged in e-commerce transactions.[135]

Under Section 7001 of E-SIGN, "a contract may not be denied legal effect, validity, or enforceability solely because an electronic signature or record was used in its formation."[136] E-SIGN defines an electronic signature as "any sound, symbol, or process attached to or logically associated with a contract . . . and executed or adopted by a person with the intent to sign the record."[137] E-SIGN

---

127. *See* Kunze, *supra* note 125.

128. S.B. No. 97 (Ca. 2001), *available at* http://www.leginfo.ca.gov/pub/bill/sen/bill/sen/sb_0051-0100/sb_97_bill_20010509_status.html (introducing a bill that would effectively repeal California's version of UETA and replace it with the NCCUSL's approved version of UETA and federal legislation).

129. *See* Saunders, *supra* note 124 (listing twenty states as having enacted UETA provisions).

130. *See* Stern, *supra* note 15, at 399 (noting that E-SIGN proponents were concerned that waiting for states to enact uniform laws could take as long as enacting other uniforms acts; for example, the UCC took approximately nine years to be accepted by most states).

131. *See* Wittie & Winn, *supra* note 58, at 297

132. Stern, *supra* note 15, at 391 (noting that in 1997 the Clinton administration urged "the private sector to respond to the public's 'wariness of conducting extensive business over the Internet because of the lack of predictable legal environment governing transactions'").

133. *See* Berman, *supra* note 24, at 144 (noting that most of E-SIGN's provision took effect in October of that same year).

134. *See* Stern, *supra* note 15, at 399 (noting that conflicting state laws requires companies "to customize their services to meet the requirements of each state").

135. *See id.*

136. 15 U.S.C. § 7001(a)(2) (2002).

137. *Id.* § 7006(5); *see also* UETA, *supra* note 72, § 2 def. 8 (defining an electronic signature to mean "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record").

does not specifically mandate that certain types of electronic signatures be used in an electronic transaction, therefore it is technology-neutral legislation.[138] In effect, an e-mail message, a digital signature, or a biometric signature can be used to execute a document, as long as it is intended to be substituted for an ink signature. Furthermore, E-SIGN's technology-neutral provisions ensure party autonomy by allowing them to choose the type of electronic signature that may be used when contracting.[139] E-SIGN's definition of electronic signature promotes e-commerce transactions because parties can use simple and inexpensive technologies to make binding agreements.

E-SIGN generates uniformity through an unusually worded preemption clause, which gives deference to state legislatures.[140] Section 7002 specifies under what circumstance state legislation will survive E-SIGN's preemption effects.[141] The preemption provision permits states to partially displace E-SIGN with UETA or equivalent legislation, which ensures "legal effect" to electronic signatures.[142] Should a state choose the latter, it may not give "greater legal status" to a particular form of electronic signature.[143] Thereafter, technology-specific state laws, such as The Utah Act are preempted by E-SIGN.[144] Furthermore, modified versions of UETA, such the California version, are also preempted by E-SIGN because they effectively exempt large numbers of state laws from UETA's grasp.[145]

---

138. *See* Jenny Oh, *Signed Sealed, Delivered, The E-Signature Act May Drive Demand For Authentication Technology*, THE INDUSTRY STANDARD, Sept. 18, 2000, *available at* http://www.thestandard.com/article/0,1902,18331,00.html?printer_friendly= (copy on file with *The Transnational Lawyer*).

139. *See* Wittie & Winn, *supra* note 58, at 300 (noting that E-SIGN protects the autonomy of the contracting parties); *see also* Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7031 (highlighting the fact that a consumer need not use electronic contracts). Additionally, E-SIGN protects consumers from inadvertently entering into electronic contracts by requiring extensive consumer consent before an electronic contract can substitute a written contract. *Id.* § 7001 (c)(1)(A)-(C).

140. *See* Wittie & Winn, *supra* note 58, at 324-25 (noting that "[i]nstead of providing, as is more common, that the Act preempts 'inconsistent' state laws or simply allowing the preemption of inconsistent state laws to be an implicit result of the supremacy clause of the Constitution, E-SIGN approaches the subject from the opposite direction").

141. *See id.* at 325.

142. *See* Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7031 (2000).

143. *See id.* § 7002(a)(2)(A)(i-ii). The Act specifies that:

> alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if—such alternative procedures or requirements are consistent with this subchapter and subchapter II of this chapter; and such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific type of technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.

Id.

144. *See* Wittie & Winn, *supra* note 58, at 334 (highlighting Congress' intention "to prevent a state from giving a leg-up or impos[ing] an additional burden on one technology or technical specification that is not applicable to all others").

145. *See* Raul et al., *supra* note 93 (citing Patricia Brumfield's discussion of §§ 1633.3(b)(4), 16.33.3(c),

E-SIGN's goal of harmonizing disjointed state electronic signature legislation is steadily being realized. Congress has not only succeeded in enacting uniform technology-neutral legislation for interstate and foreign commerce, but it has also succeeded in prompting states to adopt uniform legislation for statewide transactions.[146] Having technology-neutral legislation will be beneficial both within the United States' borders and beyond, especially if international legislatures attempt to harmonize global trade laws on electronic commerce.

C. *Harmonizing International Legislation*

The United Nations General Assembly approved the final version of the Model Law of Electronic Commerce (MLEC) in 1996.[147] The MLEC was drafted by the United Nations Commission on International Trade Law (UNCITRAL)[148] to promote the "harmonious economic relations" between nations.[149] The MLEC is a framework, which does not cover all rules and regulations, but is "intended to provide essential procedures and principles for facilitating the use of modern techniques for recording and communicating information in various types of circumstances."[150] The General Assembly believed a model law could contribute significantly to the development of harmonious international trade amongst countries with "different legal, social and economic systems."[151]

Article 7 of the MLEC addresses issues relating to electronic signatures and authentication.[152] When writing Article 7, the Working Group considered a

---

1633.3(f), 1633.5(b)-(c), 1633.15 (a)-(b) and 1633.16 from *Electronic Signatures: Impressions on California's Change to the Uniform Transaction Act*, BNA Electronic Commerce & Law Report (Dec. 1999)); *see also* Currer, *supra* note 64 (discussing the preemption effect of E-SIGN on California's version of UETA and concluding that it will be preempted to the extent it is inconsistent with E-SIGN).

146. *See* Kunze, *supra* note 125 (highlighting the fact that some forty-three states have enacted versions of UETA).

147. *See* Boss, *supra* note 57, at 1932 (discussing the initial phases that the United Nations took in addressing e-commerce).

148. *See id.* at 1947 (documenting that in 1984, UNCITRAL submitted a report to the Secretary General on the legal aspects of automatic processing). Shortly thereinafter UNCITRAL recommended that governments review the legal affects of electronic commerce. *See id.* This recommendation was endorsed by the General Assembly. *See id.* By 1986, UNCITRAL was working in the area of electronic funds transfer. *See id.* Noting that the UNCITRAL Working Group on International Payments began their work in 1987 was completed in 1992; thereafter its name was changed to the "Working Group on Electronic Data Interchange." *Id.* at 1948-52.

149. *MLEC*, *supra* note 60, at pmbl.; *see also* Boss, *supra* note 57, at 1953 (explaining that "the Model Law is intended to provide essential procedure and principles for facilitating the use of modern technique . . . in various types of circumstances").

150. Boss, *supra* note 57, at 1954.

151. *MLEC*, *supra* note 60, at pmbl.

152. *See* Boss, *supra* note 57, at 1969 (discussing the effect of Article 7 which left open a lot of judgment of the parties involved in e-commerce); *see also MLEC*, *supra* note 60, art. 7. The MLEC states in pertinent part:

> [W]here the law requires a signature of a person, that requirement is met in relation to a data message if: a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and that method is as reliable

signature's function[153] and accounted for procedures, such as stamping, which have the same binding effect as ink signatures.[154] Article 7 aims to give an electronic signature the same legal effect as an ink signature even if "it was not authenticated in a manner peculiar to paper documents."[155]

Article 7 allows an electronic signature to substitute for its ink counterpart under two conditions. First, the signer must be identifiable and there must be indicia that the signer approved the record.[156] Second, the method used to identify the signer must be appropriately reliable.[157] The requirements of Article 7 are deliberately broad in order to avoid the "risks of tying the legal framework of the [MLEC] to a given state of technological development."[158] Hence, Article 7 has a technology-neutral posture.

UNCITRAL expanded Article 7 of the MLEC by drafting a supplement to it.[159] The Working Group on UNCITRAL Model Law on Electronic Signatures (MLES)[160] specifically seeks to provide further guidance on the reliability requirement of Article 7 (1)(b) of the MLEC.[161] In formulating this section, the Working Group accounted for government participation in e-commerce transactions.[162]

---

as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

Id.

153. *See MLEC, supra* note 60, at cmt. 53 (noting signatures were used: "to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document").

154. *See id.* at cmt. 54 (noting that in some jurisdictions, "contracts for the sale of goods" above a specified value must be signed to be enforceable). However, a perforation or a typed written signature or letterhead may fulfill the requirement for a signature. *See id.*

155. *See id.* at cmt. 56 (noting that Article 7 provides "the general conditions under which data messages would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements which currently presents barriers to electronic commerce").

156. *See id.* at art. 7

157. *See id.* at cmt. 58 (listing some factors that will assist the fact finder in identifying a signer). Factors taken into account are the "sophistication of the equipment used by each of the parties . . . compliance with trade customs and practice." *Id.*

158. *See id.* at cmt. 55 (explaining the intent behind drafting Article 7).

159. *See UNCITRAL Model Law on Electronic Signatures*, UNCITRAL, 34th Sess. Annex II (2001), *available at* http://www.unictral.org/en-index.htm [hereinafter *MLES*] (copy on file with *The Transnational Lawyer*) (noting that the MLES was adopted on July 5th, 2001); *see also Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signature*, U.N. GAOR, UNCITRAL, 34th Sess., at cmt. 71, U.N. Doc. A/CN.9/493 (2001), *available at* http://www.uncitral.org/en-index.htm [hereinafter *Draft Guide*] (copy on file with *The Transnational Lawyer)* (noting that the MLES serves as a supplement to the MLEC and "is intended to provide essential principles of facilitating the use of electronic signatures"). The "main features of the [MLES] is to add certainty to the operation of the flexible standard set forth in Article 7 of the [MLEC]." *Id.*

160. *See Draft Guide, supra* note 159, at cmt. 3 (relaying a concern that divergent legislation on electronic signatures can create uncertainty); *see also* Kuner et al., *supra* note 56 (documenting the status of digital and electronic signature legislation in the European Union, North America, South America and Asia).

161. The language in Article 7(1)(b) is virtually identical to that of the Article 6(1) of the MLES.

162. *See MLES, supra* note 159, at art. 6(3). The MLES provides:

[A]n electronic signature is considered to be reliable for the purpose of satisfying the

Article 7 of the MLES suggests how to interpret a state's active participation in electronic authentication. [163] Under this article, a government agency or state-recognized private entity may choose to use specific types of electronic signatures and act as a certification authority for that electronic signature.[164] If a government prefers a particular electronic signature, then the electronic signature should automatically meet the reliability requirements of both MLEC's Article 7 and Article 6 of the MLES.[165] However, Article 7 of the MLES is not intended to exclude other types of technologies that meet the reliability requirements of the MLEC and the MLES, but it is meant to offer predictability in defining these requirements.[166]

Like the MLEC, the MLES maintains a technology-neutral approach[167] while also "adopting an approach under which the legal effectiveness of a given electronic signature technique may be predetermined."[168] However, the MLES, unlike the MLEC, was specifically drafted with the public key infrastructure in mind.[169] Thus, the MLES defines the duties and the standards of care for the signatories[170] and the certification authorities.[171]

The Working Groups from both the MLEC and MLES were cognizant of the global implementation of electronic signature legislation. The Working Group on the MLEC was influenced by entities from within the United States, such as the American Bar Association, [172] the NCCUSL, and the drafters of The Utah Act.[173]

> required to in paragraph (1) if: (a) the signature creation data are, within the content in which they are used, linked to the signatory and to no other person; (b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person; (c) any alteration to the electronic signature, made after the time of signing, is detectable; and (d) where a purpose of the legal requirement for a signature is to provide assurances as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

Id.

163. *See MLES*, *supra* note 159, at art. 7(1) (stating "[a]ny person, organ or authority, whether public or private specified by the enacting State as competent may determine which electronic signatures satisfy the provisions of Article 6 [of MLES]").

164. *See Draft Guide*, *supra* note 159, at cmt. 132.

165. *See id.* at cmt. 133; *see also MLES*, *supra* note 159, at art. 6 (noting that this section also requires that the government chosen standard be in accordance with reliable international standards).

166. *See Draft Guide*, *supra* note 159, at cmt. 133.

167. *See id.* at cmt. 5.

168. *Id.* at cmt. 4.

169. *See id.* at cmt. 133.

170. *See MLES*, *supra* note 159, at art. 8(1)(a) (requiring the signatory to "exercise reasonable care to avoid unauthorized use of its signature creation data").

171. *See id.* at art. 9(1)(b) (mandating a certification authority to "exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or which are included in the certificate").

172. *See* Boss, *supra* note 57, at 1970-71 (noting also that language in the MLEC refers to the ABA Digital Signature Guidelines).

173. *See id.* at 1970-73; *see also* Berman, *supra* note 24, at 138-54 (discussing the legislative efforts by the United States, Germany and the European Union).

Both the MLEC and the MLES maintain a technology-neutral stance[174] and lie in contrast to legislation that mandates the use of certain technologies.[175] Nevertheless, UNCITRAL has not ignored the impact of technology-specific legislation. The Working Group on the MLES seeks to define standards in which specific technologies can be utilized, while maintaining a technology-neutral approach to using electronic signatures in e-commerce.

IV. CHINA'S E-COMMERCE LEGISLATION

E-commerce, known as *Dianzi Shangwu* in Chinese, is an emerging sector of China's economy.[176] In 1999, Chinese businesses conducted $24.1 million in e-commerce sales; this figure is expected to reach $3.3 billion by 2004.[177] China's entry into the World Trade Organization will undoubtedly help it meet these forecasts.[178] However, China faces two immediate problems relating to its participation in e-commerce. First, China's national contract laws may be unable to accommodate this evolving sector of the economy because their laws do not specifically address the enforceability of electronic signatures. Second, China may not have the necessary technological infrastructure to support an expansion into the e-commerce market.[179]

The enforceability of electronic signatures in China remains uncertain because it is not explicitly addressed in China's contract law. However, significant developments regarding electronic signatures have emerged from within the financial sector[180]and from within the Chinese provincial regions.[181] These developments provide a de facto standard that will likely serve as a foundation for future national law on electronic signatures.

---

174. *See* Boss, *supra* note 57, at 1971 (reporting the MLEC's technology-neutral stance which sought legislation that worked with whatever technology the market might produce).

175. *Id.*

176. *See* JOHN WONG & NAH SOEK LING, CHINA'S EMERGING NEW ECONOMY, THE INTERNET AND E-COMMERCE 55 (2001) (discussing the growing economy as of January 2002).

177. *See id.* at 55-56.

178. *See id.* at 86; *see also* McKenzie, *supra* note 8 (noting that China's admission to the WTO should promote further e-commerce because there will be less restrictions on domestic and foreign companies to conduct business in China).

179. *See* People's Daily Online, *China Seeks Ways to Push E-Commerce*, *at* http://english.people daily.com.cn/200001/19/print20000119X122.html (last visited Nov. 10, 2001) (copy on file with *The Transnational Lawyer*) (reporting that Beijing hosted a forum on e-commerce to address issues relating to the development of infrastructure and laws relating to the Internet).

180. *See* Wang, *supra* note 9, at 21.

181. *See* WONG & LING, *supra* note 176, at 139-42.

A. Contract Law in the People's Republic of China

In 1999, China undertook measures to facilitate e-commerce by adopting the Contract Law of the People's Republic of China (PRC Contract Law).[182] Before enacting this body of law, China strongly favored traditional paper contracts.[183] Although the PRC Contract Law applies to general contract issues, such as offers and acceptance, it has roots in the MLEC.[184]

The PRC Contract Law permits parties to use digital technology to create enforceable agreements. Under Article 10, contracts can be made in forms other than written agreements.[185] Under Article 11, e-mail messages can satisfy the writing requirement because it is a physical representation of the terms of the contract.[186] However, Article 32 requires each party to "sign or affix their seal on it."[187] Herein lies the problem, as it is unclear whether an electronic signature fulfills the requirements of Article 32.[188]

Since the PRC Contract Law does not expressly address electronic signatures, contracting parties may not be able to enforce agreements executed with an electronic signature.[189] Furthermore, it is uncertain as to how, or if, an electronic signature may be admitted as evidence of a person's signature because it does not readily fit into any of the seven categories of admissible evidence in China.[190] For example, if an electronic signature is classified as "audio-visual material," it cannot stand as independent evidence and must be supported by

---

182. *See* McKenzie, *supra* note 8.

183. *See id.* (noting that this law replaced PRC Contract Laws that were drafted in the 1980s).

184. *See* Stephen Nelson & Nancy Leigh, *E-Com Legal Guide- China, at* http://www.bakerinfo.com/apec/chinaapec_main.htm (last modified Jan. 2001) (copy on file with *The Transnational Lawyer*) (discussing similar provisions for determining when a contract was formed through the use of a data messages); *see also* Wang, *supra* note 9, at 11 (explaining the procedure behind when an offers or acceptance sent electronically would become effect); *see also* Volker Pasternak, *China Could Be the Next Frontier for E-Commerce, But Investors Need Creativity and Good Nerves*, 20 No. 12 E. ASIAN EXECUTIVE REP. 9 (1998) (noting that China looked to used definitions consistent with MLEC provisions relating to electronic date interchange).

185. *See* Nelson & Leigh, *supra* note 184 (noting that written requirement is supplied through the exchange of data messages).

186. *See* Wang, *supra* note 9, at 11 (discussing, in general, the rules for electronic contract formation); *see also* McKenzie *supra* note 8 (eluding to permitted forms of electronically generated data that could be enforced under the PRC Contract Law).

187. Nelson & Leigh, *supra* note 184.

188. *See* Wang, *supra* note 9, at 12; *see also* Pasternak, *supra* note 184 (discussing the fact that provisions dealing with authentication, like those in MLEC, were not incorporated in the PRC Contract Law); *see also* Thinkquest, *Destiny, the Culture of China—Chop Engraving* (Apr. 4, 2002), *at* http://library/thinkquest.org/200443/g_chop_engraving.html (copy on file with *The Transnational Lawyer*) (describing the Chop, an object analogous to the seal, to be a traditional Chinese requirement for authenticating a person's identity).

189. *See* Nelson & Leigh, *supra* note 184 (stating that it is unclear "whether a digital signature created by asymmetric public key encryption will be recognized as the legal signature of a party because China has yet to establish a public key infrastructure to facilitate the public key encryption technology").

190. *See* Wang, *supra* note 9, at 20 n.86 (listing the other forms of admissible evidence to be "documentary evidence, material evidence, testimony of a witness, statements of a party, expert opinions, and records of inspection").

other forms of circumstantial evidence.[191] In contrast, if an electronic signature is submitted as documentary evidence, it must be an original.[192] However, in an electronic transaction the contract sent to the addressee is always a copy.[193] Chinese scholars argue that an electronic signature is admissible under either approach, as long as the data is capable of being authenticated.[194]

Although the PRC Contract Law addresses some issues relating to electronic documents, it does not expound on the legal effect of electronic signatures. The uncertainty inherent with a lack of national electronic signature legislation spawned the financial sector and provisional hubs to create their own standards.

B. The China Financial Certification Authority

The Chinese financial sector recognized the significance of e-commerce on its economy and created the China Financial Certification Authority (CFCA). The CFCA is a joint venture between twelve banks,[195] including the People's Bank of China, and serves as the root certificate authority between: banks, B2B,[196] and B2C[197] transactions.[198] The CFCA "provides security services for China's entire financial sector... [and] is becoming the security driver for China's e-commerce infrastructure."[199] Part of the CFCA's responsibility is verifying a customer's public key, thereby authenticating the customer's identity for potential clients.[200] Furthermore, this organization plans to validate approximately $1 billion worth of transactions by issuing over 100,000 digital certificates.[201] The CFCA anticipates these digital certificates will boost consumer

---

191. *See id.* at 20 (recognizing that "Chinese scholars are divided in classifying electronic messages as 'documentary evidence' or 'audio visual evidence'").

192. *See id.*

193. *MLEC*, *supra* note 60, at cmt. 62.

194. *See* Wang, *supra* note 9, at 20.

195. Press Release, Entrust, People's Bank of China (PBOC), The China Financial Certification Authority (CA) Project 2, 5 (Feb. 16, 2000) [hereinafter The CFCA Project] (copy on file with *The Transnational Lawyer*) (listing the other participating banks to be the Agriculture Bank, Industrial and Commercial Bank, Construction Bank, Communication Bank, Merchant Bank, CITIC Bank, Guandong Development Bank, Shenzhen Development Bank, Everbright Bank, Hua Xia Bank and Ming Sheng Bank).

196. The acronym B2B is used to describe transactions between businesses. Marketing terms.com, *B2B*, *at* http://www.marketingterms.com/dictionary/b2b (last visited Feb. 11, 2002) (copy on file with *The Transnational Lawyer*).

197. The acronym B2C is used to describe transactions between businesses and consumers. Marketingterms.com, *B2C*, *at* http://www.marketingterms.com/dictionary/b2c (last visited Feb. 11, 2002) (copy on file with *The Transnational Lawyer*).

198. *See* Stephanie Sim, *China Steps Up Online Banking Security*, *at* wyswyg://IDGNET_MAIN.46/http:www.secur...as_dt%3Di%26as_sitesearch%3D%26safe%3Doff (last modified Sept. 3, 2001) (copy on file with *The Transnational Lawyer*) (reporting on the CFCA's goals of providing consumers with more confidence when conducting business online).

199. *Id.*

200. *See* The CFCA Project, *supra* note 195, at 6 (describing the benefits that consumers and business will have in this venture).

201. *See Entrust, China Financial Certification Authority Tout Successful Launch of Secure Online*

confidence in business conducted over the Internet.[202] This project "is the largest e-commerce infrastructure project ever undertaken in the country" and has the central government's support.[203]

The CFCA is a beneficial institution because it provides a measure of certainty for customers who use its technology. However, the CFCA limits the type of technology parties may use to those based on public key encryption.[204] Subscribing to only one type of technology makes this a technology-specific standard. This standard has also been applied in provisional regions of China.

C. *The Shanghai Electronic Certification Authority Center*

Shanghai has taken significant steps to facilitate e-commerce and has created an infrastructure for authenticating a person's identity. On April 4, 2000, the Provisional Methods of Shanghai Municipality on the Price Management of E-Commerce (Provisional Methods) were drafted.[205] The Provisional Methods seek to manage digital certificates and to create standardized pricing for the authentication of digital certificates.[206] Under Article 4, the Shanghai Electronic Certificate Authority Center Co., Ltd. (Certificate Authority Center) is the only institution authorized to verify and authenticate a person's identity,[207] create digital certificates and manage the use of digital certificates.[208] Further, the Certificate Authority Center issues the software necessary to create digital signatures.[209] However, the Certificate Authority Center may entrust other companies to issue digital certificates.[210]

Shanghai's Provisional Methods are noteworthy for several reasons. First, the Provisional Methods were the first piece of legislation in Mainland China to

---

Banking Project, *at* http://www.entrust.cm/news/files/08_30_01_759.htm (last updated Aug. 30, 2001) (noting that the CFCA's new plan followed a pilot program which issued 15,000 digital certificates); *see also* Sim, *supra* note 198 (reporting that some CFCA officials heralded this move as "the largest effort ever undertaken to promote e-commerce in China").

202. *See* Sim, *supra* note 198.

203. The CFCA Project, *supra* note 195, at 7.

204. *See* E-mail from Carrie Bendzsa, Public Relations Manager, Entrust, Inc. to Ian Rambarran (Nov. 12, 2001, 7:37:50 PST) (copy on file with *The Transnational Lawyer*) (noting that "[t]he digital certificates will be verifying information generated by our public-key infrastructure").

205. ChinaOnline, *China's New Rules on E-Commerce Digital Certificates* (Apr. 14, 2001), *at* http://www.chinaonlince.com/reer/legal/currentnews/secure/c00040471.asp [hereinafter *New Rules*] (copy on file with *The Transnational Lawyer*).

206. *See id.* at art. 1.

207. *See id.* at art. 4 (authorizing "[t]he CA Center [to] entrust related units with the acceptance and issuing of digital certificates").

208. *See id.* at art. 5 (defining the parameters of service to include: "[o]pening new accounts: Services include customer identity verification, digital certificate creation, certification storage, certificate management, certificate inquiry, regular certificate maintenance, certificate installment and guidance for use").

209. *See id.* at art. 5(6).

210. *See id.* at art. 4.

incorporate public key cryptography into law.[211] Second, the Provisional Methods established a central role for a public body to act as a certification authority.[212] Third, the Provisional Methods are technology-specific because their service is based on public key cryptography.[213] However, the Provisional Methods fall short because they only imply official recognition of digital certificates, which in turn, could lead parties back to the unclear guidance of the PRC Contract Law to settle any disputes.[214] In contrast to Shanghai's Provisional Methods, Hong Kong has enacted extensive legislation addressing electronic signatures and e-commerce.

D. Hong Kong's E-Commerce Initiatives

Hong Kong has recognized the need to promote e-commerce and has tried to facilitate its growth by enacting legislation addressing the use of electronic signatures. In January 2000, Hong Kong implemented the Electronic Transaction Ordinance (ETO) to "facilitate the use of electronic commerce transactions for commercial and other purposes."[215] Hong Kong also enacted the Code of Practice for Recognized Certification Authorities (Code of Practice), which specifically defines the role of registered certification authorities.[216] These pieces of legislation, together, provide an enforcement mechanism for digital signatures.

The ETO allows ink signatures to be replaced by electronic signatures.[217] Specifically, the ETO mandates contracting parties use digital signatures.[218] However, the digital signature must be coupled with a digital certificate issued by a recognized certification authority.[219] Since the ETO mandates the use of only

---

211. *See* WONG & LING, *supra* note 176, at 88-97 (charting the significant the e-commerce developments in China).

212. *See New Rules*, *supra* note 205.

213. *See id.*

214. *See* Wang, *supra* note 9, at 20 (highlighting the absence of a "particular provision in the Provisional Methods stating the legal status of digital certificates, [but] they do imply . . . official recognition").

215. *See* Information Technology, *Electronic Transaction Ordinance*, *at* http://www.info.gov.hk/itbb/english/new/etcontent.htm (last updated May 5, 2000) [hereinafter ETO] (copy on file with *The Transnational Lawyer*).

216. *See* Information Services Technology Department, *Code of Practice for Recognized Certification Authorities*, *available at* http://www.itsd.gov.hk/itsd/caro/cop_pdf/cop.pdf (last modified Jan. 2000) [hereinafter *Code of Practice*] (copy on file with *The Transnational Lawyer*) (explaining that the concept for these procedures was "first articulated in the American Bar Association Digital Signature Guidelines").

217. *See* ETO, *supra* note 215, at art. 6(1) (stating that "[i]f a rule of law requires the signature of a person for certain consequences if a document is not signed by a person, a digital signature of the person satisfies the requirement but only if the digital signature is supported by a recognized certificate and is generated within the validity of that certificate").

218. *See id.*

219. *See id.*; *see also* People's Daily Online, *HK to Launch Scheme to Promote E-commerce*, *at* http://english.peopledaily.com.cn/20001/30eng2000120X101.html (last updated Jan. 30, 2001) (copy on file with *The Transnational Lawyer*) (reporting that Hong Kong is also trying to encourage its authentication infrastructure by allowing for a "voluntary certification authority"). This means that certification authorities are not required to apply for government recognition in order to provide verification services. *See id.* This move reflects the fact that Hong Kong government appreciates the role that the private sector could have in providing authentication

digital signatures and digital certificates, it is technology-specific legislation. [220]

The ETO requires the Director of the Information Technology Service Department (ITSD)[221] to give official recognition to certification authorities.[222] Subsequently, the ITSD Director officially recognized the Hongkong Post[223] as a trustworthy certification authority and charged it with the responsibility of issuing digital certificates to identify public key owners.[224] The duties of recognized certification authorities are described in detail in both the ETO[225] and its supplement, the Code of Practice.[226] Should a certification authority meet the enumerated requirements expressed in the ETO and in the Code of Practice, it will "not be liable for any loss caused by reliance on a false or forged digital signature."[227] Moreover, a recognized certification authority will not be liable for damages "in excess of the amount specified in the certificate as its reliance limit."[228] Recognizing the Hongkong Post as a certification authority appears to

---

services, and also indicates its stance away from over-regulation in this area. *See id.*

220. *See* ETO, *supra* note 215, at art. 2. Digital signature is defined by the ETO as follows:

> An electronic of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem and a has function such that a person having the initial untransformed electronic record and the signer's public key can determine: (a) whether the transformation was generated using the private key that corresponds to the signer's public key; and (b) whether initial electronic record has been altered since the transformation was generated.

Id.

221. *See* Information Technology Services Department, *Welcome, at* http://www.itsd.gov.hk/itsd/about/ewelcome.htm (last updated July 2001) (copy on file with *The Transnational Lawyer*) (reporting that the ITSD is geared to promote information technology in Hong Kong).

222. *See* ETO, *supra* note 215, at pmbl. (stating that the ETO was meant "to enable the Postmaster General to provide the services of a certificate authority and to provide for connected purposes").

223. *See* Hongkong Post, *Welcome Message, at* http://www.hongkongpost.com (last visited Feb. 24, 2002) (copy on file with *The Transnational Lawyer*) (noting that the Hongkong Post is a public entity that serves mail to the Hong Kong region.).

224. *See Government Creates Secure Environment for E-business, at* http://itsd/press/epr011204.htm (last updated Dec. 2001) (noting that the Hongkong Post is the first recognized certification authority, but in mid-2001 the ITSD recognized another certification authority); *see also* People's Daily Online, *HK Government Geared Up to Promote E-commerce, at* http://english.peopledaily.com.cn/200001/25/eng20000125X101.html (lasted updated Jan. 25, 2000) (copy on file with *The Transnational Lawyer*) (reporting that the Hongkong Post will use "public key cryptography and digital certificates" to identify parties, verify the information integrity and to ensure that electronic transactions could not be repudiated).

225. *See* ETO, *supra* note 215, at art. 37 (mandating "[a] recognized certification authority [to] use a trustworthy system in performing its services—(a) to issue or withdraw a recognized certificate; or (b) to publish in a repository or give notice of the issue of withdrawal of a recognized certificate"); *see also Code of Practice*, *supra* note 216, art. 4 (requiring certification authorities to "set out the procedures used by it . . . to authenticate a subscribers prior to the issuance of certificates" and "[describe] procedures for each class, type or description of certificates" issued by that recognized certification authority).

226. *See Code of Practice*, *supra* note 216, art. 1(1) (noting that the ITSD Director was authorized to make these provisions under ETO art. 33).

227. ETO, *supra* note 215, at art. 42(1).

228. *Id.* at art. 42(2) (specifying that this safe harbor provision could be waived by the certification authority).

be part of a strategy aimed at developing a public certification authority.[229]

In contrast to Mainland China, Hong Kong has extensive legislation regarding electronic signatures. The ETO mirrors prior legislative acts once favored in the United States. For example, the ETO provides explicit duties for certification authorities, similar to those in The Utah Act.[230] In addition, the ETO is technology-specific, only allowing a digital signature coupled with a digital certificate to be as enforceable as an ink signature.[231] Like The Utah Act, the ETO does not explicitly authorize any other forms of technology that could be used for authentication. The ETO's technology-specific posture contrasts with E-SIGN and MLEC, as these regulations have technology-neutral language.

Although China's national contract law addresses some issues relating to e-commerce transactions, it falls short of addressing electronic signatures. Nevertheless, interest in electronic signatures has not been ignored. The CFCA, the Provisional Methods, and the ETO have created an infrastructure within which digital signature technology can be used. Furthermore, the government officials in both Shanghai and Hong Kong are trying to elaborate their existing infrastructure by creating a cross-certification system to allow these regions to accept digital certificates from each other.[232] However, the benefits provided are limited to transactions either executed within those regions or within the banking industry.

V. THE FUTURE OF CHINESE E-COMMERCE LEGISLATION

Chinese initiatives in the financial sector and within the provisional areas reveal several themes that will likely influence any future legislation addressing electronic signatures. However, these underlying themes may be contrary to laws similar to E-SIGN and MLEC. Nevertheless, the Chinese legislature should consider the examples set by both E-SIGN and MLEC so that the strengths and weaknesses of each can be compared to those of technology-specific legislation, such as The Utah Act.

---

229. *See* China Daily Information, *Digital Signature Framework to Boost E-commerce*, *at* http://www.chinadaily.com.cn/cover /storydb/2000/09/30/it-cnidigital.html (last modified Sept. 30, 2000) (copy on file with *The Transnational Lawyer*) (reporting that the first step is to provide the "legal framework for the development of a public key infrastructure . . . The second prong is the establishment of a public certification authority, and the third is for the government to adopt a public key infrastructure").

230. *See* Utah Code Ann. §§ 46-3-201, 46-3-301(d), 46-3-309(2)(a) (2001).

231. *See id.* § 46-3-403; *see also* Berman, *supra* note 24, at 139.

232. *See* Hongkong Post e-Cert, *Cooperation Arrangement between HK Post and Shanghai Electronic Certification Authority*, *at* http://www.info.gov.hk/gia/general/200105/24/0523310.htm (last updated May 24, 2001) (copy on file with *The Transnational Lawyer*) (reporting that this arrangement will ultimately explore "the development of a Chinese Certification Authority System for Hongkong Post").

A. *Underlying Themes in China's E-commerce Legislation*

There are two themes tying the CFCA, the Provisional Methods, and the ETO together. First, the government or an official body plays a central role in issuing digital certificates. Second, each subscribes to a technology-specific approach and has a bias towards public key cryptography. However, a new trend may be emerging that contrasts with these commonalities.

The CFCA, the Provisional Methods and the ETO each call for a central governmental role in electronic transactions. The Provisional Methods, for example, authorizes the Certificate Authority Center to be the only entity in Shanghai permitted to issue digital certificates and provide authentication services.[233] Likewise, the ETO requires a digital signature to be accompanied by a digital certificate issued by a state recognized certification authority.[234] The central control theme exists for two reasons. First, the Chinese government mistrusts the use of encryption because they fear parties might use it to circumvent the government's ideology or compromise its national security interests.[235] Second, China wants to ensure that consumers deal with trustworthy certification authorities so that they are not dissuaded from participating in the e-commerce marketplace.[236]

The second underlying theme between the CFCA, the Provisional Methods and the ETO is their subscription to public key cryptography. The CFCA and Shanghai's Certificate Authority Center have both based their authentication services on digital certificates made with public key cryptography.[237] Furthermore, the ETO also requires parties to use both digital signatures and digital certificates based on public key cryptography.[238] Thus, the CFCA and the

---

233. *See New Rules*, *supra* note 205, art. 4.

234. *See* Angus Forsyth & Yvonne Chia, *How Contract Law Applies to Cyberspace and the Pitfalls Posed by the Electronic Transactions Ordinance, at* http://www.hk-lawyer.com/200-6/June0)0-79.htm (last visited Feb. 16, 2002) (copy on file with *The Transnational Lawyer*) (noting that digital certificates issued by unrecognized certification authorities are unenforceable under the ETO).

235. *See* John Eichelberger & Annabel Allen, *A Legal Perspective: The Impact of the WTO on Foreign Investment in China's Internet/E-Commerce Sector, at* http://www.perkinscoie.com/resource/intldocs/to impact.htm (last visited Aug. 28, 2001) (copy on file with *The Transnational Lawyer*) (highlighting the Chinese government's concern that the Internet could be used to disseminate state secrets); *see also* Wang, *supra* note 9, at 19 (reporting that in October 1999, China required "all foreign and domestic firms or individuals using encryption technology to register with the government"). However, this mandate was eventually modified because U.S. trade lobbyists moved the Chinese State Encryption Administration Commission to exclude application of this law to wireless telephones and Windows applications. *See id.*

236. *See* Information Technology Service Department, *Government Creates Secure Environment for E-Business, at* http://www.itsd.gov.hk/itsd/press/epr011204.htm (last modified Apr. 12, 2001) (copy on file with *The Transnational Lawyer*) (quoting Mr. Alan Wong, Director of Information Technology Services Department (ITSD) who said "[w]ithout trust, the community will not have the necessary confidence that makes transactions on-line possible"). Also, Mr. Wong noted that the ITSD is seeking to identify vulnerable parts of their information infrastructure so they may be protected from cyber attacks. *See id.*

237. *See* The CFCA Project, *supra* note 195, at 6-7.

238. *See* ETO, *supra* note 215, at art. 6(1).

legislative acts in both Shanghai and Hong Kong adhere to a technology-specific approach to electronic authentication.

On the other hand, there is evidence suggesting that a future Chinese law on electronic signatures may contain technology-neutral language. For example, the Chinese have based parts of their PRC Contract Law on segments of the United Nations' MLEC.[239] Moreover, Chinese scholars have declared that Chinese e-commerce law should conform to the general provisions of the United Nations.[240] Finally, recent ventures between public entities have moved away from using only digital signatures and have adopted the use of other electronic signatures, such as those based on biometric technology.[241]

China's underlying themes of government participation and preferences for public key cryptography are well established. However, being mindful of developments occurring outside its borders offers alternatives to the Chinese status quo, and should be a factor when considering what style of legislation works best in China.

B. Trying to Find the Legislative Mold that Fits in China

China is essentially faced with three types of electronic signature legislation. First, is the technology-specific style of legislation modeled after The Utah Act. Second, is the purely technology-neutral example set by E-SIGN. Third, is the technology-neutral approach with adaptations for government participation, as exemplified by both MLEC and MLES. When molding a law that best caters to China's needs, the Chinese legislatures should test each of the aforementioned examples with the underlying themes mentioned above.

Should Chinese legislatures follow examples of technology-specific legislation, like The Utah Act, it might be able to readily fulfill its goals. First, technology-specific legislation offers the Chinese government a measure of central control by mandating parties to use a specific technology. Furthermore, the central control theme can also be maintained by requiring a state body to issue digital certificates or have a private business do the same, as long as they meet the Chinese security requirements.[242] In addition, the Chinese government's participation in e-commerce should build the public's confidence because state bodies offer a measure of security.[243] Finally, having a technology-specific body of national legislation will build on the infrastructure already in place within

---

239. *See supra* note 184 and accompanying text.

240. See Pinxin, *supra* note 11.

241. *See* UVentures, *Nanjing Civic Bureau Signs Licensing Agreement with Cic China for Electronic Signatures* (May 14, 2001), *available at* http://www.uventure.com/servlets/UVTechNews/2590 (copy on file with *The Transnational Lawyer*) (noting that the trend amongst Chinese organizations to employ the most current advances in electronic signature technology).

242. *See id.* (noting that "[t]he Chinese government's general policies toward the internet and e-commerce are a blend of encouragement and control).

243. *See* Sim, *supra* note 198.

China. Thus, any Chinese legislative action similar to The Utah Act should readily satisfy the underlying themes previously discussed.

If China enacts technology-neutral legislation similar to E-SIGN, it will be unable to preserve the two themes of central control and technology-specific legislation. For example, a Chinese law mandating that digital signatures be used would immediately clash with E-SIGN because it forbids giving greater legal status to electronic signatures.[244] Also, requiring parties to use government issued digital certificates as a prerequisite to enforcing a digital signature, would collide with E-SIGN because it prohibits the preferential treatment of electronic signatures.[245] The alternative is to allow parties to use any electronic signature and use the services from any certification authority. This predicament is the opposite result to the central control theme exemplified above. Furthermore, excluding the Chinese government from participating as a certification authority could reduce the public's confidence when contracting online.[246]

If China enacts technology-neutral electronic signature legislation similar to MLEC and MLES, it could still maintain the themes mentioned above. The MLEC and MLES are technology-neutral, and both essentially allow any electronic signature to be used instead of an ink signature. However, the electronic signature must both identify the contracting party, and be made through a "reliable" method.[247] To fulfill the reliable method requirement, MLES contemplates a country appointing a public entity to determine which electronic signatures are reliable.[248] To maintain a measure of central control, China may create a public certification authority, like the Shanghai's Certificate Authority Center, and give it the ability to automatically deem digital signatures as reliable. Further, the public certification authority can offer verification services. Thereafter, the consumer confidence goal is also maintained because public certification authorities will be available to consumers and businesses. Under MLEC and MLES, other types of electronic signatures are not per se unenforceable; rather, the burden of proof is higher because parties must show the particular electronic signature used is reliable.[249] Thus, a Chinese law following the approach suggested by the United Nations could be both technology-neutral and maintain the two themes of central control and a preference for specific technologies.

Technology-specific legislation may readily fit China's immediate needs, more so than technology-neutral models of legislation. Although legislation like

---

244. *See* 15 U.S.C. § 7002(a)(2)(A) (2002); *see also id.* § 7006(d) (allowing any form of electronic signature to replace an ink signature as long as the party's intent is clear); *see also* UETA, *supra* note 72, art. 2 def. 8 (interpreting the term electronic signature to mean "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record").

245. *See* § 7002 (a)(A)(2)(A).

246. *See* Sim, *supra* note 198.

247. *MLEC*, *supra* note 60, art. 7.

248. *See MLES*, *supra* note 159, art. 8.

249. *See Draft Guide*, *supra* note 159, at cmt. 133.

E-SIGN departs from the established practices already in place within China, legislation like the MLEC and MLES could incorporate China's immediate needs. However, subscribing to either the model exemplified by the United States or the model enunciated by the United Nations would require the government to have a "hands off" approach to electronic authentication. Nonetheless, the benefits of technology-neutral legislation should not be ignored.

C. Factors and Suggestions for Formulating Electronic Signature Legislation in China

When formulating electronic signature legislation, China should consider the development of legislative acts promulgated outside its borders. Moreover, China ought to consider the underlying policies that led to the development of technology-specific and technology-neutral acts. By looking to other legislative initiatives, China can identify the benefits and the weaknesses of each and mold any future national legislation accordingly. Subsequently, China may find the approach taken by MLEC and MLES could serve its interests best.

Considering the development of electronic signature legislation and noting the policies behind those laws will inevitably assist China when formulate its own legislation. First, China must consider what type of legislation will promote e-commerce transactions. Second, China needs to contemplate whether the presumed security benefits of any technology-specific legislation will continue to exist after new technologies develop. Third, Chinese legislatures must note that higher transaction costs could be imposed on consumers because parties must purchase software, hardware and verification services of third parties to meet the demands of technology-specific legislation. Fourth, the Chinese have to consider whether or not preserving party-autonomy could be beneficial to an emerging economy. Fifth, China needs to consider whether the incentives to develop new technologies will be reduced in the electronic authentication industry by mandating the use of certain technologies. Finally, the Chinese legislature must discuss whether mandating technology-specific legislation would overly burden it to act and create new legislation when old technologies become obsolete and new measures become necessary.

China should adopt legislation to facilitate e-commerce, but the legislation should also be flexible enough to accommodate developing technologies. By assimilating a law with a technology-neutral posture, China will promote e-commerce because parties can use various types of electronic signatures. If the Chinese adopt a technology-neutral law it should facilitate more e-commerce than a technology-specific law because parties have a greater incentive to participate in e-commerce when they need not purchase peripheral services for low valued transactions. Although the security benefits of a technology-neutral law may be lower on average than the alternative, parties could still secure their

transactions by choosing more reliable forms of authentication when necessary.[250] Also, a technology-specific law could prove to be problematic for China in the future because any mandated technology may become obsolete and insecure as new technologies develop. This could result in the Chinese government sponsoring unreliable technologies that may injure the public's confidence when conducting business over the Internet. Alternatively, the Chinese legislature will have to reformulate legislation after new technological developments and this situation could prove impractical. Thus, it seems that the benefits associated with technology-specific legislation are outweighed by the benefits of technology-neutral legislation.

China should adopt a technology-neutral law because it allows the greatest flexibility for parties and promotes the use and development of electronic signatures. A law similar to the suggestions from the United Nations could prove to be better suited for the Chinese, than a law modeled after E-SIGN, because both the MLEC and MLES have a more accommodating approach to government participation in e-commerce transactions. If China enacts technology-specific legislation, like The Utah Act, which mandated the use of only digital signatures, it will be discordant with countries that have incorporated versions of the MLEC and the MLES into their law and also be inconsistent with its most valued trading partner, the United States.[251]

V. CONCLUSION

There are two significant facts relating to China as of January 2002. First, China has not enacted national e-commerce legislation legalizing the use of electronic signatures in contracts. Second, China has been admitted to the World Trade Organization. Combined, these will impact China's position in the global e-commerce market. To take advantage of e-commerce and to create legal certainty, China needs to implement a scheme of national legislation explicitly recognizing the use of electronic signatures. Although the trend in China is tilted towards technology-specific legislation, there are signs that China may implement technology-neutral legislation.

Nevertheless, without explicit direction regarding electronic signatures, the ease in which they can be used to execute transactions across thousands of miles will not be successfully utilized.

---

250. *See* discussion *supra* Part II.A (discussing the security risks associated with e-mails when compared to digital signatures or biometric signatures).

251. *See* People's Daily Online, *supra* note 9 and accompanying text. *See also* Kuner et al., *supra* note 56 (noting that Japan also has a technology-neutral legislation).