CHINA'S NEW ELECTRONIC SIGNATURE LAW AND CERTIFICATION AUTHORITY REGULATIONS: A CATALYST FOR DRAMATIC FUTURE GROWTH OF E-COMMERCE

Stephen E. Blythe*

China's E-Commerce: Getting Ready for a Boom

Estimates put China's population at approximately 1.3 billion people.[1] Yet only 1.03 million of them[2]—less than eight percent of the population[3]—have access to the internet. This will soon change. The dizzying annual growth rate of the economy[4] has begun to create a new middle class in China. Recent reports indicate an 8.6 percent rise in real disposable income among urban households.[5] That middle class is expected to grow to 170 million households by 2010.[6] By the end of this decade, the number of people wired to the internet in China will exceed that of the United States,[7] and China will become the world's largest online market.[8]

In 2005, China's electronic commerce ("e-commerce") business is expected to approach $620 billion.[9] In the 2006-2007 year, eBay expects online sales to China to grow at an astounding rate of sixty-one percent per year.[10] It is going to be a boom. The market is huge, and

* Professor of Law and Accounting, School of Management, New York Institute of Technology, CERT Technology Park, P.O. Box 5464, Abu Dhabi, United Arab Emirates. Ph.D. Candidate (Law), The University of Hong Kong; Ph.D. (Business Administration), University of Arkansas, 1979; J.D. *cum laude*, Texas Southern University, 1986; LL.M. (Int'l Bus. Law) University of Houston, 1992; LL.M. (Info. Tech. Law) *with distinction*, University of Strathclyde (Scotland), 2005. Attorney at Law, Texas and Oklahoma; C.P.A., Texas.

[1] CIA, CHINA, THE WORLD FACT BOOK, (last visited Oct. 25, 2005), https://www.cia.gov/cia/ publications/ factbook/geos/ch.html.

[2] CHINA INTERNET NETWORK INFORMATION CENTER, 16TH STATISTICAL SURVEY REPORT ON THE INTERNET DEVELOPMENT IN CHINA (July, 2005), at 5, *available at* http://www.cnnic.org.cn/download/2005/2005072601.pdf. Another source recently estimated that a lesser number of people—only 87 million—currently have internet access in China. *See*, Karen Lowry Miller, *Asia Bound*, *NEWSWEEK*, Oct. 18, 2005, *available at* http://www.msnbc.msn.com /id/6199775/site/newsweek/print/1/displaymod.

[3] 103,000,000 / 1,306,313,812 = 7.88 %.

[4] Dragon Venture: All About China Business Newsletter (April 2005), *available at* http://www.dragonventure. com/ En/2005-04/newsletter_index.shtml.

[5] *Id.*

[6] Door Martyn Williams, *EBay Lauds China's E-Commerce Potential*, WEBWEREL, Feb. 11, 2005, http://www.webwereld.nl /articles/30637.

[7] *Id.*

[8] Tim Richardson, *China Set for Ecommerce Boom*, THE REGISTER, Jan. 17, 2005, http://theregister.co.uk /2005/ 01/17/china_ ecommerce/print.html. In 2006, China experienced its greatest annual increase in the number of internet users to date, an increase of 23.4% over 2005. *See Internet usage in China hits record high*, C/NET NEWS. COM, Jan. 23, 2007, http://news.com.com/2102-1032_3-6152408.html?tag=st.util.print.

[9] APEC: E-Commerce Business Alliance, *Alibaba Acquires Yahoo China*, Aug. 17, 2005, http://www.apec-ecba.org/ english/info/Article.jsp?a_no=189&col_no=10&dir=200508&siteid=english. Currently, there are 20 million online sellers in China. *See* APEC: E-Commerce Business Alliance, *China Boasts of 20 Million E-commerce Dealers*, Aug. 17, 2005, http://www.apec-ecba.org/english/info/Article.jsp?a_no=301&col_no=9&dir=200509&siteid=english.

[10] Miller, *supra* note 2, at 1. The Chairwoman of the China E-Commerce Association, Ms. Song Ling, was only slightly less sanguine in her forecast. Speaking in April at the 8th Annual E-Commerce Conference in Beijing, she

the potential return on investment is high. The *modus operandi* of American firms' entrance into e-commerce in China seems to be proven U.S. internet firms buying local Chinese internet firms that already have an understanding of the market and a firm foothold in it; ordinarily, U.S. firms do not undertake e-commerce activity in China on their own.[11] Three cases in point will illustrate this phenomenon: (1)Yahoo paid $1 billion to enter into a venture with Alibaba.com, a Hong Kong-based firm, and they plan to develop a Chinese-language search engine which will compete with Google,[12] and last spring, Yahoo formed another venture with Sina.com, China's largest internet website, to get a piece of the action in the online auction business; (2) eBay purchased a Chinese auction website firm (Eachnet) in 2002 and has recently integrated it with its global network, investing $150 million more in the venture; and (3) Amazon, settling for a smaller share of the auction pie, purchased Joyo.com for $72 million in August.[13] Yet, the potential market is so huge that there may be room for all of them to succeed. However, eBay's CEO, Meg Whitman, is keen on becoming the undisputed winner in China.[14] The stakes are high; Ms. Whitman says, "[w]hoever wins China, will win the world."[15]

Despite the tremendous boom now forecast, a number of factors have burdened the development of e-commerce in China up to now. Most Chinese people like cash and are unaccustomed to using "plastic money."[16] Only thirty-eight percent of online buyers pay with credit or debit cards.[17] As a result, bicycle-borne couriers often deliver cash payment to the vendor,[18] buyers may use a bank or the post office to wire the money,[19] or purchases may be made C.O.D.[20] Credit rating systems are underdeveloped and unreliable.[21] All too often, postal service is slow and unpredictable.[22]

However, there has been a more pervasive, more fundamental reason for China's often insecure and unreliable payment systems. Before 2005, no national e-commerce law existed in China to either mandate or promote the utilization of relatively more secure payment systems. Fortunately, that omission has been recently rectified. On April 1, 2005, the first comprehensive e-commerce law went into effect in China. It includes an Electronic Signature Law ("ESL")[23] as

---

predicted a growth rate of 50 percent this year. *See* CRIENGLISH.com, *China's E-Commerce to Grow 50%*, Apr. 17, 2005, at 1, http://en.chinabroadcast.cn/2600/2005-4-18/154@228632.htm.

[11] Miller, *supra* note 2.

[12] *Id. See also E-commerce Key to China Web Growth: Dotcom Guru Jack Ma Speaks to CNN*, Oct. 26, 2005, http://edition.cnn.com/2005/TECH/10/19/spark.jack.ma/; Andrew Orlowski, *Yahoo! Buys! Into! Chinese! Ecommerce! Giant!*, THE REGISTER, Aug. 10, 2005, http://www.theregister.co.uk/2005/08/10/yahoo_china

[13] *Id.*

[14] *Id.*

[15] Bruce Einhorn, *A Cooler Look at Yahoo in China*, E-COMMERCE TIMES, Sept. 27, 2005, at 3, http://www.ecommercetimes.com/story/46322.html.

[16] *Id.*

[17] Miller, *supra* note 2, at 1.

[18] *Id.*

[19] Robert D. Hof, *EachNet: Bringing E-Commerce to China*, BUSINESS WEEK ONLINE, Mar. 15, 2004, at 1, http://www.businessweek.com/magazine/content/04_11/b3874020.htm?chan=search.

[20] Richardson, *supra* note 8, at 2. Two-thirds of E-commerce transactions are paid for C.O.D. or by post office wire transfers.

[21] Miller, *supra* note 2, at 1.

[22] *Id.*

[23] Order (No. 18) of the President of the People's Republic of China, LAW OF THE PEOPLE'S REPUBLIC OF CHINA ON ELECTRONIC SIGNATURE (hereinafter "Electronic Signature Law," or "ESL"), Adopted at the 11th

well as Certification Authority Regulations. [24] In enacting this landmark statutory and administrative law, China has positioned its e-commerce market for a launch into an arguably inevitable ride to the heights. Because of the new law, e-commerce customers now have access to more secure and trusted payment systems. This should act as a catalyst to the internet marketplace and propel it to an even more dazzling degree of success than it would otherwise have achieved.

Objectives of the Article

The objectives of this article are to (1) give the reader an appreciation for the burgeoning potential of e-commerce in China; (2) concisely describe the basic aspects of public key infrastructure technology and digital signatures and explain their impact on e-commerce transactions; (3) cover China's new electronic signature ("e-signature") law and compare it to e-signature laws of other jurisdictions; (4) cover China's new regulations pertaining to Certification Authorities ("CAs") and compare them with their counterparts in other jurisdictions; and (5) make recommendations for improving China's e-signature law and CA regulations.

I. Electronic Signature Laws

Three generations of e-signature laws have appeared since 1995. The first mandated the utilization of only the digital signature, and no other form of e-signature. The second reversed the first and took an open-minded attitude toward allowance of any type of e-signature. The third adopted a moderate position between the two extremes of the first and second, recognizing many forms of e-signatures but granting preferred status to the digital signature.

A. The First Wave: Technological Exclusivity

An e-signature is "any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with the intent to authenticate a writing."[25] There are many forms of e-signatures; examples include "a name typed at the end of an e-mail message, a digitized fingerprint, a digitized image of a handwritten signature attached to an electronic

---

Meeting of the Standing Committee of the Tenth National People's Congress of the People's Republic of China, Promulgated Aug. 28, 2004, Effective April 1, 2005. The translation is available (by subscription only) at: http://www.lawinfochina.com/ dispecontent.asp?db=1&id=3691 (last visited Oct. 25, 2005).

[24] Order (No. 35) of the Ministry of Information Industry of the People's Republic of China, MEASURES FOR THE ADMINISTRATION OF ELECTRONIC CERTIFICATION SERVICES (hereinafter sometimes "Certification Authority Regulations" or "CAR"), Adopted at the 12th Executive Meeting of the Ministry of Information Industry of the People's Republic of China, Promulgated 28 January 2005, Effective April 1, 2005. The Beijing University School of Law, Beijing, China, translated the CAR into English. The translation is available (by subscription only) at: http://www.lawinfochina.com/dispecontent.asp?db=1&id=4002 (last visited Oct. 25, 2005).

[25] Jochen Zaremba, *International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers*, 18 CONN. J. INT'L L. 479, 511 (2003). Chinese law defines an "electronic signature" as "the data included and attached in data message in electronic form, for the use of identifying the identity of the signatory and showing that the signatory has recognized the contents therein." ESL, *supra* note 23, art. 2.

message,[26] a retinal scan, a PIN number, or a digital signature."[27] Perhaps the most sophisticated type of e-signature is the "digital signature."

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an ESL.[28] The Utah statute gave digital signatures legal recognition, but did not do the same for other types of e-signatures.[29] The authors of the Utah statute believed, with some justification, that digital signatures provide the greatest degree of security for electronic transactions. Utah was not alone in this attitude; other jurisdictions that grant exclusive recognition to the digital signature include India,[30] Germany, Italy, Malaysia and Russia.[31]

Unfortunately, these jurisdictions' choice of "technological-exclusivity" is burdensome and overly-restrictive.[32] Forcing users to employ digital signatures gives them more security, but this benefit may be outweighed by the digital signature's disadvantages—more expense, less convenience, more complication and less adaptability to technologies used in other nations, or even by other persons within the same country.[33]

B. The Second Wave: Technological Neutrality

Jurisdictions in the second wave of ESLs overcompensated. They completely reversed the first wave and did not include any technological restrictions whatsoever in their statutes. They did not insist upon utilizing digital signatures or any other form of technology to the exclusion of other types of e-signatures. These nations have been called "permissive" because they take a completely open-minded, liberal perspective on e-signatures and do not contend that any one of them is necessarily better than the others. In other words, they are technologically-neutral. Examples of permissive jurisdictions include the United States, the United Kingdom,[34] Australia and New Zealand.[35] Permissive jurisdictions legally recognize many types of e-signatures and do not grant a monopoly to any specific one.

---

[26] Chinese law defines a "data message" as "the information created, sent, received, or stored by such means as electron, optics, magnetism or the similar means." ESL, *supra* note 23, art. 2. The ESL is rather technologically-neutral and recognizes that messages may be transmitted with a variety of technologies.

[27] Zaremba, *supra* note 22.

[28] UTAH CODE ANN. § 46-3-101 et seq. (1999).

[29] *Id.*

[30] Stephen E. Blythe, *A Critique of India's Information Technology Act and Recommendations for Improvement*, 33 SYRACUSE J. INT'L. L. & COMMERCE (2007).

[31] Susanna Frederick Fischer, *California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation*, "Association of American Law Schools 2001 Annual Meeting, Section on Law and Computers, 7 B.U. J. SCI. & TECH. L. 229, 234 (2001).

[32] *Id.*

[33] It is debatable whether technology-neutrality or technology-specificity is the correct road to take. *See* Sarah E. Roland, Note, *The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?*, 35 SUFFOLK U. L. REV. 625, 638-45 (2001).

[34] For concise coverage of American and British digital signature law, *see* Stephen E. Blythe, *Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security*, 11RICH. J. L. & TECH. 6, 7 (2005).

[35] Fischer, *supra* note 31.

The disadvantage of the permissive perspective is that it does not take into account that, in fact, some types of e-signatures *are* better than others. A PIN number and a person's name typed at the end of an e-mail message are both forms of e-signatures, but neither even approaches the degree of security that the digital signature provides.

C. The Third Wave: Moderate Degree of Technological Neutrality

Singapore was in the vanguard of the third wave. This country adopted a compromise, middle-of-the-road position with respect to the various types of e-signatures. The UNCITRAL Model Law on Electronic Commerce influenced Singapore's lawmakers.[36] In terms of relative degree of technological neutrality, Singapore adopted a "hybrid" model. This model prefers the digital signature because of its legal presumption of reliability and security, but not to the exclusion of other forms of e-signatures.[37] Singapore did not want to become "hamstrung" by tying itself to a one form of technology.[38] The Singapore legislators realized that technology is continually evolving and that it would be unwise to require one form of technology to the exclusion of others.[39] In other words, the Singapore statute gives the digital signature more respect, but does not grant it a monopoly, as does the Utah statute. Singapore allows use of other types of e-signatures. This technological open-mindedness is commensurate with a global perspective and allows parties to consummate electronic transactions with parties from other nations with greater ease.

D. China Joined the Third Wave

The drafters of the Chinese statute weighed all of these factors and chose the Singapore-style, moderate position.[40] This hybrid approach is also the one taken by the European Union's E-Signatures Directive,[41] Iran,[42] Pakistan,[43] Japan,[44] Vanuatu,[45]Taiwan,[46]Lithuania,[47] South Korea,[48] Barbados,[49] Hong Kong,[50] Bermuda,[51] Dubai,[52] Tunisia,[53] Azerbaijan[54] and Bermuda.[55]

---

[36] United Nations Commission on International Trade Law ("UNCITRAL"), MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT (hereinafter "MLEC"), G.A. Res. 51/162, U.N. GAOR, 51ST Sess., Supp. No. 49, at 336, U.N. Doc. A/51/49 (1996), http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf. *See* Stephen E. Blythe, "Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality," 33 OHIO NO. U. L. REV. ___ (2007).

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] Zhang Chu and Lingfei Lei, *The Chinese Approach to Electronic Transactions Legislation*, 9 COMP. L. REV. & TECH. J. 333, 343-47 (2005).

[41] COUNCIL DIRECTIVE 1999/93/EC, 2000 O.J. (L 13) 12; *See* Stephen E. Blythe, *supra* note 30. For discussion of the Hungarian implementation of the EU Directive, *see* Stephen E. Blythe, *Hungary's Electronic Signature Act: Enhancing Economic Development With Secure E-Commerce Transactions*, 15 INFO. & COMM. TECH. L. 47-71 (2007), a publication of Routledge Publishing Co., a member of the Taylor & Francis Group, *available at* http://www.tandf.co.uk/journals/journal.asp?issn=1360-0834&linktype=5.

[42] Islamic Republic of Iran, ELECTRONIC COMMERCE LAW OF THE ISLAMIC REPUBLIC OF IRAN, http://irtp.com/laws/ec/IR%20Iran%20E-Commerce%20Law.pdf. *See* Stephen E. Blythe, *Tehran Begins to Digitize: Iran's E-Commerce Law as a Hopeful Bridge to the World*, SRI LANKA J. INT'L. L. (2006).

[43] Stephen E. Blythe, *Pakistan Goes Digital: The Electronic Transactions Ordinance as a Facilitator of Growth for E-commerce*, ISLAMIC STATE PRACTICES IN INT'L. L. (2006), *available at* http://electronicpublications.org/catalogue.php?id=46.

[44] Stephen E. Blythe, *Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access*, J. INTERNET L. 20-26 (2006).

Deleted: .

E. Attributes of a Digital Signature System

Under its new statute, China grants a degree of privileged-status to the digital signature. Hence, it is appropriate at this point to consider some of the characteristics of a digital signature system. If the parties to an e-commerce transaction decide to use a digital signature, there is a need for two underlying technologies and a third party: (1) asymmetric cryptology; (2) public key infrastructure ("PKI"); and (3) a Certification Authority ("CA").[56]

F. Asymmetric Cryptology

Under the Utah Model, digital signatures receive legal protection "only if asymmetric key cryptology produced the digital signature."[57] Such a system employs double keys—the sender uses one key to encrypt the message, and the recipient uses a different, albeit mathematically related,[58] key to decrypt the message.[59] Senders have a private key, known only to them used to generate the digital signature, and the recipient uses the public key, often available online, to

---

[45] Stephen E. Blythe, *South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga*, J. SOUTH PACIFIC L. (2006), *available at* http://www.paclii.org/journals/fJSPL/vol10 _2006.shtml.

[46] Stephen E. Blythe, *Taiwan's Electronic Signature Act: Facilitating the E-Commerce Boom With Enhanced Security*, a paper presented and published in the PROCEEDINGS OF THE SIXTH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON BUSINESS, Honolulu, Hawaii U.S.A., May 25-28, 2006, available at http://www.hicbusiness.org/Proceedings_Bus.htm .

[47] Stephen E. Blythe, *Lithuania's Electronic Signature Law: Providing More Security in E-Commerce Transactions*, 8 BARRY L. REV. (2007).

[48] Stephen E. Blythe, *The Tiger on the Peninsula is Digitized: Korean E-Commerce Law as a Driving Force in the World's Most Computer-Savvy Nation*, 28: 3 HOUS. J. INT'L L. 573 (2006).

[49] Stephen E. Blythe, *The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute*, 16 CARIBBEAN L. REV. (2007).

[50] Before amending its original digital signature law, Hong Kong only recognized digital signatures and was therefore a member of the First Wave. After amendments were made, Hong Kong joined the Third Wave. *See* Stephen E. Blythe, *Electronic Signature Law and Certification Authority Regulations of Hong Kong: Promoting E-Commerce in the World's "Most Wired" City*, 7 N.C. J. L. & TECH. 1 (2005).

Deleted:

[51] Fischer, *supra* note 28, at 234-37.

[52] Stephen E. Blythe, *The Dubai Electronic Transactions Statute: A Prototype for E-Commerce Law in the United Arab Emirates and the G.C.C. Countries*, 22:1 JOURNAL OF ECONOMICS AND ADMINISTRATIVE SCIENCES (2007) *available at* http://jeas.cbe.uaeu.ac.ae/.

[53] Stephen E. Blythe, *Computer Law of Tunisia: Promoting Secure E-Commerce Transactions With Electronic Signatures*, 20 ARAB L. Q. 317-344 (2006), *available at* http://www.ingentaconnect.com/content/brill/alq.

[54] Stephen E. Blythe, *Azerbaijan's E-Commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region*, 1:1 COLUMBIA J.EAST EUROPEAN L. (2007).

[55]Fischer, *supra* note 28, at 234-37.

[56] Richard Wu, *Electronic Transaction Ordinance—Building a Legal Framework for E-commerce in Hong Kong*, 2000:1 J. INFO. L. & TECH. 5-9 (2000), *available at* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_1/wu/.

[57] Renard Francois, Comment, *Fair Warning, Preemption and Navigating the Bermuda Triangle of E-Sign, UETA, and State Digital Signature Laws*, 19 J. MARSHALL J. COMPUTER & INFO. L. 401, 405-06 (2001).

[58] American Bar Association ("ABA"), *PKI Assessment Guidelines*, V 0.30 at 301 (Public Draft for Comment No. 25, 2001), *available at* http://www.abanet.org/scitech/ec/isc/pagv30.pdf.

[59] By contrast, "symmetric" cryptology employs one key. The same key is used for both encryption and decryption. Thus, the sender and recipient are using the same key. There are two disadvantages: (1) two stranger-parties using a public network have no way to securely transmit symmetrical keys to be used in subsequent transmissions; and (2) the transfer of a key in such a situation could possibly be intercepted or modified by a third party. *See* Robin C. Capehart & Mark A. Starcher, *Wired, Wonderful West Virginia: Electronic Signatures in the Mountain State*, 104 W. VA. L. REV. 303, 311-312 (2002).

verify that the proper party created the message and that it has not been altered during transmission.[60] This is a very good system for e-commerce, since two stranger-parties, perhaps living far apart, can confirm each other's identity and thereby reduce the likelihood of fraud in the transaction.

G. Public Key Infrastructure

Before a party can digitally "sign" anything, he or she must first be in possession of a pair of keys—the private key and a related public key.[61] The party must apply to a CA[62] to confirm his or her identity. After the CA confirms the applicant's identity, the CA will issue the pair of keys, and a certificate[63] as verification of the subscriber's identity. The CA places the certificate in a public repository, most often the CA's website. Whenever the subscriber[64] digitally signs a message, the CA confirms the signature of the sender;[65] the CA then informs the recipient of the encrypted message which public key is necessary to decode the message.[66] At that point, the recipient is able to access the public key, the decryption code which the recipient uses to read the sender's encrypted message.[67]

The Utah model prescribes an open PKI system.[68] In an open system, all parties with whom the subscriber wants to transact use the same certificate. Accordingly, it is relatively easier

---

[60] ABA, *Section of Science & Technology, Information Security Committee, Electronic Commerce & Information Technology Division, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (ABA Net, 1995 and 1996), *available at* http://www.abanet.org/ftp/pub/scitech/ds-ms.doc.

[61] Aristotle Mirzaian, Esq., *Electronic Commerce: This is Not Your Father's Oldsmobile*, 26 RUTGERS L. REC. 7, 13 (2002).

[62] China law refers to a Certification Authority as an "electronic certification service provider," and defines it as a "third party institution that provides electronic signatories and electronic signature dependents [relying third parties] with electronic certification services for electronic signature[s]." CAR, *supra* note 24, art. 2. This article prefers to call them Certification Authorities ("CA") because that designation is used in the United States and many other international jurisdictions. The service provided by the CA is deemed to be "public." *Id.* Hence, its regulation by the government is justified. The purpose of the CA is to verify that the E-signatures of its subscribers are authentic and reliable. *See also* ESL, *supra* note 23.

[63] China law refers to a certificate as an Electronic Signature Certification Certificate (hereinafter "certificate"). This article uses the one-word reference because it is used more internationally. China's definition of a subscriber (Electronic Signature Certification Certificate) is "the data message or other electronic records that can prove that any electronic signatory has any connection with the data made by electronic signature." ESL, *supra* note 23, art. 34(3).

[64] China law refers to a subscriber as an "Electronic Signatory." An Electronic Signatory is defined as "the person who holds data made by electronic signature and implement electronic signature in his own identity or on behalf of the person he represents." ESL, *supra* note 23, art. 34(1). This article uses the term "subscriber" because it is used more commonly used internationally.

[65] China law defines Electronic Signature Validation Data as "the data used for validating electronic signature, including codes, passwords, arithmetics (*sic*) or public keys, etc." ESL, *supra* note 23, art. 34(5).

[66] Michael H. Dessent, *Digital Handshakes in Cyberspace Under E-Sign: 'There's A New Sheriff in Town!*, 35 U. RICH. L. REV. 943, 992 (2002). China law states that data made by an electronic signature (e.g., character, coding, etc.) may be used to "connect [an] electronic signature with [an] electronic signatory reliably." ESL *supra* note 23, art. 34(4).

[67] Jane Kaufman Winn, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, 37 IDAHO L. REV. 358, 384-88 (2001).

[68] Richard Wu, *supra* note 56, at 8. In a closed PKI system, the user-subscriber must obtain a different certificate for different groups of people with whom they want to conduct transactions with. The advantage is that legal liability is potentially more limited, since the CA and members of a certain group may enter into agreements defining their

to enter into a transaction because it is easier to sign a document digitally.[69] However, if the subscriber's private key is lost or compromised, the consequences are potentially much more egregious because there is a greater likelihood that the subscriber may be defrauded.[70]

H. Certification Authorities

China uses a compulsory system to regulate CAs.[71] No firm may engage in CA activities unless the government of China has issued it a license.[72] The Ministry of Information Industry ("MII") is the national governmental agency designated to license and to regulate CAs.[73] For CAs to be effective, subscribers, relying third parties,[74] and the general public needs to trust[75] and be willing to place reliance in the CA.[76] In China, the ESL helps effectuate the CA by specifying stringent requirements for the issuance of the CA license.[77] In order to qualify, the CA must convince the MII that it uses a trustworthy system of issuing and withdrawing certificates, and of displaying them in a public repository.[78] The MII has issued CA regulations that contain the general policies, procedures and rules that CAs must employ to implement the ESL. The CA regulations must be understood and followed by the CA.[79] Furthermore, every CA is required to write and submit a report (called a Certification Practice Statement, hereinafter "CPS") to the MII clearly outlining the specific procedures and rules that have been implemented in issuing certificates and in carrying out its other tasks.[80] The MII has a number of enforcement powers that it may exercise against CAs.[81] For example, the MII may revoke a CA's license if they do not maintain a trustworthy system,[82] or abide by the provisions of the ESL, the Certification Authority Regulations ("CAR"), or their own CPS.

---

rights and responsibilities toward each other; in an open PKI system, public law defines the rights and responsibilities of the parties. On the other hand, the disadvantage of the closed PKI system is that it is relatively more difficult than the open system to digitally sign a document and to enter into a transaction. *Id.* at 8-9.

[69] *Id.* at 8, citing D.J. Greenwood, *Risk and Trust Management Techniques For an "Open but Bounded" Public Key Infrastructure*, 38 JURIMETRICS J. 277 (1998).

[70] Benjamin Wright has argued forcefully that PKI does not result in the elimination or even the reduction of risk; it simply transfers it to the private key. In a PKI system, it is critical for the private key holder to keep it secret and to maintain security over it. Although a sophisticated party involved with "high-end financial deals" may appreciate the advantages of the PKI system, the unsophisticated person may be uncomfortable in being responsible for the all-powerful private key. *See* Symposium: Cyber Rights, Protection, and Markets, *Eggs in Baskets: Distributing the Risks of Electronic Signatures*, 32 U. WEST. L.A. L. REV. 215, 219-220 (2001).

[71] Other jurisdictions (e.g., Hong Kong) use a "voluntary" regulatory program for its CA's. In voluntary systems, it is possible for a firm to engage in CA work without a license. However, there are disadvantages in doing so, particularly the inability to limit the liability of the firm. *See* Stephen E. Blythe, *supra* note 45.

[72] CAR, *supra* note 24, art. 4.

[73] ESL, *supra* note 23, art. 25.

[74] Under China law, a relying third party is referred to as a "Party Depending on Electronic Signature" (hereinafter "relying third party") and is defined as "the person who undertakes the relevant activities on the basis of his trust on any electronic signature certification certificate or electronic signature." ESL, *supra* note 23, art. 34(2). This article prefers "relying third party" because that phrase is more popular internationally.

[75] For an article pertaining to the attainment of trust in E-commerce in China, *see* Timothy L. Fort & Liu Junhai, *Chinese Business and the Internet: The Infrastructure for Trust*, 35 VAND. J. TRANSNAT'L L. 1545 (2002).

[76] CAR, *supra* note 24, art. 18.

[77] ESL, *supra* note 23, art. 17.

[78] CAR, *supra* note 24, art. 17.

[79] CAR, *supra* note 24.

[80] ESL, *supra* note 23, art. 19; *see also* CAR, *supra* note 24, art. 34.

[81] CAR, *supra* note 24, art. 36-40.

[82] ESL, *supra* note 23, art. 33.

In reaction to the government's desire to maintain security for state secrets, and the concern of e-commerce parties over security of private information, the ESL included a provision mandating secrecy.[83] Official secrets must not be divulged.[84] Persons attaining access to confidential data while performing functions covered by the ESL (e.g., the CA acquires a subscriber's personal information during an application for a certificate[85]) are prohibited from disclosing it to other persons.[86] The ESL also forbids disseminating false information whilst engaged in a function under the statute (e.g., giving false information to a CA in an application for a certificate),[87] or pretending to be a CA.[88] Violators may be subject to fine or imprisonment.[89]

II. The Background of E-Commerce Law in China

Before the appearance of the ESL and the CAR in 2005, Chinese e-commerce law was influenced by federal contract law, rules of the banking industry, and provincial and municipal e-commerce law.

A. The Contract Law of 1999

Prior to the enactment of the new ESL, e-commerce parties relied on the general Contract Law of 1999 ("Contract Law")[90] for authority. The Contract Law recognizes that contracts may be concluded in "written, oral or *other forms*."[91] "Other forms" is significant because it opened the door to consideration of the validity of the electronic form.

Under the Contract Law, if the parties have agreed that the contract in writing, then that agreement controls.[92] However, the next article implies that information stored in digital form is "equal" to information stored in writing.[93] An e-mail message may fulfill the writing requirement because it physically conveys the contractual terms and can show the described content "visibly." However, this only provided "simple" equivalency.[94] The United Nations Commission on International Trade Law, in its Model Law for Electronic Commerce ("MLEC"),[95] called for e-commerce laws of the world to recognize the "functional" equivalency of digital information in

---

[83] CAR, *supra* note 24, art. 20.
[84] ESL, *supra* note 23, art. 15.
[85] *Id.* at art. 18.
[86] CAR, *supra* note 24, art. 20.
[87] ESL, *supra* note 23, art. 20.
[88] *Id.* at art. 29.
[89] *See generally* Paul Toscano, *Toward an Architecture of Privacy for the Virtual World*, 19 J. MARSHALL J. COMPUTER & INFO. L. 151 (2000).
[90] Ninth National People's Congress (Second Session), CONTRACT LAW OF THE PEOPLE'S REPUBLIC OF CHINA (hereinafter "Contract Law"), Adopted 15 March 1999. The Contract Law was translated into English by the Beijing University School of Law, Beijing, China, and is available at: http://lawinfochina.com/dispfree.asp?b=1&id=1080&keyword=contract,1999.
[91]. ESL, *supra* note 23, at art. 10. (Emphasis added).
[92] *Id.*
[93] *Id.* at art. 11.
[94] Fuping Gao, *The E-Commerce Legal Environment in China: Status Quo and Issues*, 18 TEMP. INT'L & COMP. L.J. 51, 55 (2004).
[95] MLEC, *supra* note 32.

electronic form, which consists of three elements: (1) "simple" equivalency—that an electronic record is equal to a writing; (2) that an e-signature is equal to a written signature as required by law; and (3) that an electronic record has the same legal status as an original record, if specified criteria are met.[96] Because it failed to address the second and third items, the Contract Law did not convey how electronic records would serve the functions of a paper document. Accordingly, the Contract Law failed to fulfill the legal needs of parties engaged in e-commerce in China.

Article 32 states that the contract does not come into existence until the parties "sign or affix their seal on it."[97] This statement leaves room for ambiguity. Articles 11 and 32 seem to be in conflict; the former allows e-mail messages to qualify as written form, but the latter establishes a rule that a contract will not come into existence until the parties have signed or sealed it.[98] The problem is this: since e-mail messages are neither signed nor sealed, it is debatable as to whether an e-signature complies with Article 32.[99]

Nevertheless, the Contract Law contains some sound authority for the recognition and validity of electronic contracts in China.[100] For example, several of its Articles specify when and where electronic contracts are formed:

1. Ordinarily, an offer becomes effective when the offeree receives it.[101] However, if a contract is negotiated electronically, the time at which the offer becomes effective is determined as follows: (a) if the offeree has designated a specific computer system under his control for the offer to be sent to, the time the offer enters that system will be the time the offer becomes viable; but (b) if the offeree has *not* designated a specific computer system under his control as the one for the offer to be sent to, the time the offer enters any computer system under the control of the recipient will be the time that the offer becomes viable.[102]

2. Ordinarily an acceptance becomes effective when the offeror receives it.[103] (This assumes that it is a bilateral contract. For unilateral contracts, see Rule 3, below.) However, if a contract is negotiated electronically,[104] the time at which the acceptance—and the contract—becomes effective is determined as follows: (a) if the offeror has designated a specific computer system under his control for the acceptance to be sent to, the time the acceptance enters that system will be the time the acceptance (and the contract) becomes viable; but (b) if the offeror has *not* designated a specific computer system under his control as the one for the acceptance to be sent to, the time the acceptance enters any computer system under the control of the offeror will be the time that the acceptance, and the contract, become viable.[105]

---

[96] Fuping Gao, *supra* note 96.
[97] *Id.*
[98] *Id.*
[99] Ian A. Rambarran, Comment, *I Accept, But Do They? The Need for Electronic Signature Legislation on Mainland China*, 15 TRANSNAT'L L. 405, 426 (2002).
[100] *Id.*
[101] CONTRACT LAW, *supra* note 90, art. 16, par. 1.
[102] *Id.* at art. 16, par. 2.
[103] *Id.* at art. 26, par. 1. There is no "Mailbox" Rule in China.
[104] In the English translation, the Contract Law refers to electronic messages as "data-telex." *Id.* at art. 16, par.2.
[105] *Id.* at art. 26, par. 2, citing CONTRACT LAW, art. 16, ¶2.

3. In the case of a unilateral contract, the offeree accepts with action, not words.[106] Therefore, the acceptance and the contract become viable when the offeree performs an act of acceptance "in accordance with transaction practices or as required in the offer."[107]

4. If the contract is negotiated using e-mail messages, one party may require the other to execute a confirmation letter before the contract is formed.[108] If so, the contract will come into existence when the confirmation letter is executed.[109]

5. Ordinarily, a contract will be considered to have come into existence at the place the acceptance occurred.[110] However, if a contract is negotiated electronically, the acceptance is assumed to have occurred at the "main business place" of the recipient.[111] If the recipient has no business place, it will be considered to have occurred at the recipient's residence.[112]

6. The parties have latitude to make their own agreement as to the assumed place at which their contract comes into existence, notwithstanding Rule 5, above.[113]

Unfortunately, the Contract Law of 1999 did not consider the validity and enforceability of e-signatures.[114] Furthermore, e-signatures did not fit easily and naturally into any of the seven categories of admissible evidence in China, so it was debatable whether e-signature evidence was admissible in court.[115] Nevertheless, if authentic, e-signature are potentially admissible under two categories of evidence: "audio-visual" or "documentary."[116] For e-signatures to fall under audio-visual, the party would have to provide circumstantial evidence to support the introduction of the e-signature.[117] On the other hand, if a party introduces an e-signature as "documentary" evidence, it would have to be an original, since copies are not acceptable.[118] The problem created here is that the recipient of a contract in e-commerce necessarily receives only a copy—not the original.[119]

B. The Banking Industry's China Financial Certification Authority

Often, developments in the private sector precede the creation of law by the government. Such was the case of e-signature Law in China. Realizing the need for the issuance of e-signatures, the banking industry was proactive and created a joint venture of twelve banks (including the People's Bank of China), calling itself the China Financial Certification Authority ("CFCA"). They began to issue digital certificates in reference to (1) bank-to-bank transactions;

---

[106] "Unilateral Contract," LAW.COM DICTIONARY, http://www.law.com (search for term "unilateral contract").
[107] CONTRACT LAW, *supra* note 90, art. 26.
[108] *Id.* at art. 33.
[109] *Id.*
[110] *Id.* at art. 34.
[111] *Id.* at art. 34, ¶2.
[112] *Id.*
[113] *Id.*
[114] Rambarran, *supra* note 99, at 426.
[115] *Id.*
[116] *Id.* at 426-27.
[117] *Id.*
[118] *Id.* at 427.
[119] *Id.*

(2) business-to-business transactions; and (3) business-to-consumer transactions. Their plans included the validation of more than $1 billion of transactions through the issuance of more than 100,000 digital certificates. The CFCA issued only digital certificates and used PKI exclusively.[120]

C. The Emergence of E-Commerce Law at the Municipal and Provincial Levels

Chinese e-commerce law originated at the municipal and provincial levels, not at the federal level.

1. Municipal Law: Shanghai Electronic Certification Authority Center

In 2000, sensing the need for law pertaining to e-commerce, the Shanghai City Government adopted an ordinance designed to manage e-commerce.[121] This ordinance created a governmental CA, the Shanghai Electronic Certificate Authority Center Co., Ltd., which became the only institution in Shanghai authorized to engage in the following CA activities: (1) verifying a person's identity; (2) creating and managing digital certificates; and (3) issuing the software necessary to create digital certificates.[122] However, the ordinance did not mandate that the Center remain a CA monopoly in Shanghai It also gave the Center the authority to entrust other firms to become CA's.[123]

The Shanghai law was the first legislation in China to require the utilization of PKI technology (and thereby technological-specificity); and establish a governmental CA.[124] However, the Shanghai law did not extend official legal status to digital certificates, which forced a reliance on the ambiguous national Contract Law.[125] Nevertheless, the Shanghai ordinance was an important step in the evolutionary development of e-commerce law in China.

2. Provincial Law

Governments in the provinces were mindful of the e-commerce developments. They began to take action. Hainan Province and Guangdong Province led the way in the passage of e-commerce law.

a. Hainan

In August 2001, Hainan became the first province to issue digital signature rules—the *Interim Measures for the Administration of the Certification of Digital Certificates*.[126] The

---

[120] Shanghai Municipal Informatization Commission, http://www.shanghaiit.gov.cn/englishweb/index.htm; Rambarran, *supra* note 99, at 427-28.
[121] Rambarran, *supra* note 99, at 428.
[122] *Id.*
[123] *Id.*
[124] *Id.* at 428-29.
[125] *Id.*
[126] Hainan Provincial People's Government, INTERIM MEASURES FOR THE ADMINISTRATION OF THE CERTIFICATION OF DIGITAL CERTIFICATES (August 9, 2001); Perkins & Coie, *Hainan Leads the Way With Digital Signature Rules*, CHINA LEGAL HIGHLIGHTS (October 2001), http://www.perkinscoie.com/content /en/updates/china/october 2001.htm.

Interim Measures defined basic terms[127] and established a governmental agency, the Hainan Information Industry Administration, to regulate CA's.[128] The law specifies the CA licensing procedure, the CA's services and liabilities, and the content and standards pertaining to digital certificates.[129]

b. Guangdong

The Congress of Guangdong Province issued its *Ordinance on Electronic Transactions* in December 2002.[130] Significantly, the Guangdong Ordinance became the one of the first laws to provide legal authority in court for eradicating barriers to utilizing electronic transactions.[131] The Guangdong Ordinance covers e-signature issues as well as CA issues.[132] The provincial government of Guangdong established a public CA—the Guangdong Electronic Certification Authority.[133]

III. China's Electronic Signature Law

The Electronic Signature Law ("ESL")[134] was enacted and disseminated on August 28, 2004[135] and was implemented on April 1, 2005.[136] According to China's Ministry of Justice, the writers of the ESL considered the following sources in the drafting process: legal and e-commerce experts, the UNCITRAL Model Law on Electronic Commerce,[137] the UNCITRAL Model Law on E-Signatures,[138] the European Union's E-Commerce Law,[139] the European Union's E-Signatures Directive,[140] and e-signature statutes of the United States,[141] Japan,[142] Korea,[143] Singapore,[144] and other countries.[145]

---

[127] Perkins & Coie, *supra* note 126. The defined terms included: electronic document, digital signature, digital certificate, and digital certificate certification authority.
[128] *Id.*
[129] *Id.*
[130] Zhang Chu and Lingfei Li, *supra* note 35, at 336; *Guangdong Unveils China's First Draft Law on E-Commerce*, TDCTRADE.COM (November 15, 2001); http://www.tdctrade.com/alert/cba-e0111b.htm; Andrew Zheng, Perkins & Coie, Beijing, *E-commerce in China—Guangdong Promulgates Comprehensive Legislation*, http://www.perkinscoie.com/page.cfm?id=51.
[131] Chu and Li, *supra* note 35, at 336-37.
[132] Gao, *supra* note 96, at 57.
[133] *Digi-Sign and Guangdong Electronic Certification Authority Cooperate on Unified-Cert Service*, Hong Kong, 18 May 2004, *available at* http://www.tradelink.com.hk/eng/20040518.html. The Guangdong Electronic Certification Authority ("GECA") now has more than 180,000 subscribers; its website address is http://www.cnca.net. On 18 May 2004, GECA announced it had entered into a cooperative agreement with Digi-Sign, a Hong Kong CA, to jointly issue a "Unified-Cert." The Unified-Cert makes it possible for Mainland China residents (possessing valid travel documents to Hong Kong, or a Hong Kong Identity Card) to simultaneously obtain, in one application, both the digital certificate of GECA and Digi-Sign's ID-Cert. This service is expected to lead to an increase of online activities between Guangdong Province and Hong Kong. .
[134] ESL, *supra* note 23.
[135] *Id.* at preface.
[136] ESL, *supra* note 23, at preface and art. 36.
[137] MLEC, *supra* note 32.
[138] United Nations Commission on International Trade Law, UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES (2001), 32 Y.B. U.N. Comm'n Int'l Trade L. 499, U.N. Doc. A/CN.9/SER.A/2001, *available at* http://www.uncitral.org/en-index.htm.
[139] COUNCIL DIRECTIVE 2000/31/EC, 2000 O.J. (L 178) 1.
[140] COUNCIL DIRECTIVE 1999/93/EC, 2000 O.J. (L 13) 12.

The ESL was enacted for these reasons: (1) to grant e-signatures the same legal status as the handwritten or sealed signature; (2) to regulate the procedures undertaken when using e-signatures; and (3) to delineate the rights and responsibilities of the parties, i.e., the subscriber, the CA, and relying third parties.[146]

In private, civil matters, the parties are free to agree on whether they will or will not use e-signatures or data messages.[147] The ESL does not compel any party to contract electronically in a private agreement. That is a private decision for the parties to make.

Documents created using e-signatures or data messages, if agreed to by the parties, are just as legally binding as "hard copy" documents.[148] The ESL forbids parties to contest their legal status based on the mere fact that they were created using e-signatures or data messages.[149]

The ESL requires the traditional "hard" copy in these special cases:[150] (1) family-related documents (e.g., marriage, divorce, adoption, wills, etc.);[151] (2) documents pertaining to transfer of real estate;[152] (3) documents relating to canceling public utility services (e.g., electricity, water, natural gas, telephone, TV cable);[153] and (4) other instances as determined by applicable laws or regulations.[154]

The ESL covers data messages, rules of evidence, e-signatures, and liabilities of the parties; those issues are presented in that order.

A. Data Messages

---

[141] UNIFORM ELECTRONIC TRANSACTIONS ACT, 7A U.L.A. 23 (2002 & Supp. 2004). *See* Stephen E. Blythe, *supra* note 30.
[142] Japan, LAW CONCERNING ELECTRONIC SIGNATURES AND CERTIFICATION SERVICES (24 May 2000), *available at* http://www.meti.go.jp/english/report/data/gesignconte.html. *See* Stephen E. Blythe, *supra* note 44.
[143] Republic of South Korea, DIGITAL SIGNATURE ACT (1999, amended 2001), a*vailable at* http://site.securities.com/94dec/Data/KR/klri/B5505792.html. *See* Blythe, *supra* note 48.
[144] Republic of Singapore, ELECTRONIC TRANSACTIONS ACT (1998), *available at* http://statutes.agc.sg/. *See* Blythe, *supra* note 36.
[145] Ministry of Justice, LEGISLATIVE DEVELOPMENTS, August 28, 2004, *available at* http://www.legalinfo.gov.cn/english/LegislativeDeve/legislativedeve2_25.htm . One of the principal drafters of the ESL, and a member of the consulting board advising the drafters, contend that the most influential information sources were: UNCITRAL Model Law on E-Commerce of 1996, the UNCITRAL Model Law on E-Signatures, and the E-signature law of Singapore. *See* Chu and Lei, *supra* note 35, at 344-47.
[146] ESL, *supra* note 23, art. 1.
[147] *Id.* at art. 3
[148] *Id.*
[149] *Id.*.
[150] *Id.*
[151] *Id.* at art. 3(1).
[152] *Id.* at art. 3(2).
[153] *Id.* at art. 3(3).
[154] *Id.* at art. 3(4).

Deleted:

If a law or a regulation mandates that pertinent information be recorded in writing, the ESL states that utilization of a data message will suffice if it includes the same contents, and is just as accessible, as a paper document.[155]

In order for a data message to have the same legal status as an original, it must (1) be capable of accurately communicating the contents of the original; (2) have the ability to be retrieved for use at any time; and (3) provide assurance that the contents are complete and unaltered from the time they were created.[156]

In assessing whether the data message has integrity vis-à-vis the original, it is irrelevant that the data message may contain an endorsement or have its form altered during "data interchange, storage, and display."[157]

If a law or a regulation mandates retaining a document in a repository, the document may be in the form of a data message if (1) the data message contains the same information, and is just as accessible, as a paper document; (2) either the format of the data message is same as when it was "created, sent, or received,"[158] or, despite a different format, it is still able to convey the original contents; and (3) it identifies the addresser and the addressee of the data message, and its dispatch and receipt times.[159]

B. Rules of Evidence

The ESL contains several rules pertaining to admitting a data message into evidence in a court of law The mere fact that the evidence is in the form of a data message, with no extenuating circumstances, is an insufficient ground for excluding the evidence.[160] In other words, just because information was created, sent, or received as a data message is not enough to prevent the information from being admitted into evidence in court.[161] Of course, just because information in the form of a data message has been admitted into evidence does not guarantee that the information is accurate. Factors to be considered by the court in assessing the veracity of information in a data message include: (1) whether the methods used in creation, storage, or transmission of the data message were reliable; (2) whether the methods used to maintain integrity of the contents were reliable; (3) whether the methods used to identify the addresser were reliable; and (4) other factors which may be relevant in the particular case.[162]

C. Data Message Assumed Sent by Addresser

The ESL presumes in any of the following situations that the message in question emanated from its addresser: (1) the message was sent after the addresser authorized it to be sent; or (2) it was sent automatically by the addresser's computer information system; or (3) using the

---

[155] *Id.* at art. 4.
[156] *Id.* at art. 5.
[157] *Id.*
[158] *Id.* at art. 6(2).
[159] *Id.* at art. 6.
[160] *Id.* at art. 7.
[161] *Id.*
[162] *Id.* at art. 8.

validation method prescribed by the addresser, the addressee determines that the data message is valid.[163] Notwithstanding the above, the parties are free to negotiate different rules and to stipulate them in their contract.

D. The Time and Place of Transmission and Receipt of Messages

If a law or regulation mandates a sender to confirm receipt of a data message, or if the parties have so stipulated, the ESL requires that the sender confirm.[164] If the sender has received any confirmation from the recipient, then the ESL assumes that the recipient received the data message.[165]

The ESL assumes the sender sent the message at the time it first entered into an information system outside the control of the sender.[166] If the recipient has designated a specific information system to send the message to, then the ESL assumes the recipient received the message at the time it entered said system.[167] Alternatively, if the recipient does not designate a specific information system, then the ESL assumes the recipient received the message at the time it first entered into any system under the control of the receiver.[168] However, if the parties have different stipulations regarding the time of sending or receiving, then the stipulations will control.[169]

The ESL assumes the message was sent from the sender's primary business address, and the message was received at the recipient's primary business address.[170] If a party has no primary business address, then it assumes that the person's habitual residence was the sending or receiving place.[171] However, if the parties have stipulated which sending or receiving address to assume, then the stipulation will control.[172]

E. E-Signatures and Their Certification

This section explores the interrelation among: reliability of an e-signature, the subscriber's duties, and the CA.

1. Characteristics of a Reliable E-Signature

Because of the heightened level of its security, the ESL grants reliable e-signature the same legal status as the handwritten signature, or signing with a seal.[173]

---

[163] *Id.* at art. 9.
[164] *Id.* at art. 10.
[165] *Id*
[166] *Id.* at art. 11.
[167] *Id.*
[168] *Id.*
[169] *Id.*
[170] *Id.* at art. 12.
[171] *Id.*
[172] *Id.* The ESL rules pertaining to time and place in which a message is sent or received are in agreement with the rules set out in the Contract Law, but they are not as comprehensive as the Contract Law rules. Hence, it appears the Contract Law rules remain applicable to E-commerce in some situations, e.g., when one party requires the other to sign a confirmation letter. CONTRACT LAW, *supra* note 90, art.33.
[173] ESL, *supra* note 23, art. 14.

In order to be considered "reliable," an e-signature must simultaneously meet all of the following requirements: (1) all data generated in the e-signature process is used exclusively by the e-signature, and the e-signature's sole owner is the subscriber; (2) the data generated by the e-signature is controlled exclusively by the subscriber when signing; (3) any modification of the e-signature after signing is discoverable by the subscriber; and (4) any modification of the form or contents of the data message is discoverable by the subscriber after signing.[174]

The parties may also elect to use the e-signature under reliable conditions, in compliance with their stipulations.[175]

2. Subscriber's Duty to Protect and to Inform

The subscriber has a duty to the other parties to protect the data that the e-signature has generated. If the subscriber becomes aware that the security of such data has been or may become compromised, the subscriber should immediate stop using such data and notify all other relevant parties (i.e., the CA and relying third parties) immediately.[176]

3. The Certification Authority

The Certification Service Provider, as mentioned in the ESL, is often referred to in other jurisdictions as the CA. The purpose of the CA is to provide a third-party verification of the authenticity of an e-signature. In China, only an organization licensed by the MII, the designated regulatory agency of the national government, can provide CA services.[177]

4. The CA Application Procedure

The prospective CA organization must file an application with the MII[178] and submit relevant documentary evidence[179] showing that (1) it has sufficient suitable personnel—both technicians and managers—to engage in the CA business; (2) it possesses sufficient capital and has a place of business suitable for the CA business; (3) it possesses sufficient equipment and technology that is in compliance with the national safety standards; (4) it has certification documents with codes approved by the appropriate government agencies; and (5) it meets all other legal and regulatory requirements.[180]

Upon receipt of an application, the MII must undertake an investigation of the applicant to ascertain whether it qualifies to be a CA.[181] The MII must consult with the commerce department on the matter.[182] Within 45 days, the MII must make a decision.[183] If the decision is

---

[174] *Id.* at art. 13.
[175] *Id.*
[176] *Id.* at art. 15.
[177] *Id.* at art. 16. For elaboration of the CA's functions, *see* CAR, *supra* note 24, art. 17.
[178] *Id.* at art. 18.
[179] *Id. See also* CAR, *supra* note 24, art.6.
[180] ESL, *supra* note 20, art. 17. More specificity of these items is provided in the CAR, art. 5 *infra.*
[181] ESL, *supra* note 20, art. 18.
[182] *Id.*
[183] *Id.*

positive, the MII will issue the license.[184] If the decision is negative, the MII will not issue the license,[185] and the MII must inform the applicant, explaining the reasons for the negative decision.[186]

5. Requirements of New CAs

Upon receiving the license, the new CA must register as a business enterprise at the department of commerce.[187]

The MII requires the new CA to post the following on the CA's website: name of entity, license number, and other relevant information.[188]

Additionally, the MII mandates the new CA to write its "business rules," to file them with the MII, and to disseminate them to the public on the CA's website.[189] This statement of business rules (hereinafter, "CPS"[190]) must include the following information: (1) extent of liabilities, and to whom; (2) operational matters and specifications; (3) measures taken to protect the information under the CA's control; and (4) other matters that the MII may determine.[191]

6. Application of Subscriber to CA for Certificate

Subscribers are legally bound to provide full and accurate information to the CA when applying for a certificate.[192] In turn, the CA is legally required to check the validity of the subscriber's identification and the accuracy of the information submitted in the application.[193]

7. Information Required on Certificates

Before issuance, the CA must carefully check all certificates for accuracy to eliminate any mistakes.[194] Each and every certificate must contain the following items: (1) name of the CA organization; (2) name of the subscriber; (3) serial number of the certificate; (4) the date the certificate becomes valid and the date it expires; (5) the e-signature "validation data"[195] of the subscriber; (6) e-signature of the CA; and (7) other items that the MII may be determine.[196]

---

[184] *Id.*
[185] *Id.*
[186] *Id.*
[187] *Id.*
[188] *Id.* Additional information to be published by the new CA is mentioned in the CAR, art. 12 *infra*. Also, the MII will give public notice of the issuance of the new license. *See* CAR art. 10 *infra.*
[189] ESL, *supra* note 20, art. 19. *See also* CPS *infra,* art. 15-16.
[190] In other jurisdictions (e.g., Hong Kong and the United States), this list of operating rules is referred to as the "Certification Practice Statement," (or "CPS"), and that is the designation used in this article. For a detailed analysis of the Hong Kong CA Regulations pertaining to preparation of the CPS, *see* Blythe, *supra* note 50.
[191] ESL, *supra* note 20, art. 19.
[192] *Id.* at art. 20.
[193] *Id.*
[194] *Id.* at art. 21.
[195] *Id.* This is the subscriber's "public key."
[196] *Id.* The CA also has an obligation to inform the certificate applicant several categories of information. CAR, *supra* note 24, art. 21.

8. CA's Duty to Keep Relying Parties Informed

The CA has a legal duty to maintain the accuracy of information contained in the certificate during the period of its validity.[197] The CA must ensure that relying third parties are aware of relevant matters pertaining to the certificate and are able to prove the accuracy of information contained in the certificate.[198]

9. Voluntary Termination of the CA's Business

If a CA decides to go out of business, it must inform all affected parties (i.e., the subscriber and relying third parties) at least ninety days before the proposed termination date.[199] At least sixty days before the proposed termination date, the CA must inform the MII, and begin negotiations for another CA to take over the business activities of the departing CA.[200] In the event the departing CA is unable to find another CA to assume its business activities, it must so inform the MII, who will then designate another CA to take over the departing CA's business.[201]

10. Involuntary Termination of the CA's Business

If the MII revokes the CA's license to do business, the CA has no obligation to locate another CA to take over its business operations.[202] In that situation, the MII will handle all matters pertaining to finding of another CA to assume the revoked CA's business operations.[203]

11. Retention Requirement

A CA has the responsibility to retain all documents and information related to certificates it has issued for a period of five years after the invalidation of the certificate.[204]

12. Oversight by MII

China's Ministry of Information Industry is the administrative department designated to provide oversight of the CAs, in accordance with the ESL and the CAR.[205]

13. Reciprocal Recognition of Foreign CAs

China affords certificates issued in a foreign country, by a foreign CA, the same legal status as domestically issued certificates, provided that the MII approves the recognition, and a reciprocity agreement exists between China and the foreign country in question, or the recognition is justified because of reciprocity principles.[206]

---

[197] ESL, *supra* note 23, art. 22.
[198] *Id. See also* CAR, *supra* note 24, art. 18.
[199] ESL, *supra* note 23, art. 23; *see also* CAR, *supra* note 24, art. 24(1).
[200] ESL, *supra* note 23, art. 23; *see also* CAR, *supra* note 24, art. 23 and art. 24(2).
[201] ESL, *supra* note 23, art. 23; *see also* CAR, *supra* note 24 art. 25.
[202] ESL, *supra* note 23, art. 23; *see also* CAR, *supra* note 24, art. 26.
[203] *ESL, supra* note 23, art. 23; *see also* CAR, *supra* note 24, art. 26.
[204] ESL, *supra* note 23, art. 24. The length of the retention period varies from jurisdiction to jurisdiction. For example, it is seven years in Hong Kong. *See* Blythe, *supra* note 45.
[205] ESL, *supra* note 23, art. 25.
[206] ESL, *supra* note 23, art. 26; *see also* CAR, *supra* note 24, art. 42.

F. Liabilities of the Parties

The ESL imposes liabilities upon the subscriber, the CA and relevant government officials.

1. Liability of the Subscriber

The subscriber shall be liable for payment of compensatory damages to relying third parties in the following situations: (1) when the subscriber does not provide full and truthful information to the CA; (2) when the subscriber knows that any data made by an e-signature has either exposed official secrets or possibly may expose official secrets, but the subscriber fails to notify the other parties and stop them from utilizing the data; and (3) when the subscriber has been at fault in any other manner.[207]

2. Liability of the CA

The CA may incur legal liability in three situations.

a. Failure to Inform of Inaccurate Information in Certificate

The CA shall be liable for payment of compensatory damages to the subscriber, and to relying third parties when the other parties have been harmed by utilizing the CA's service.[208] To avoid this liability, the burden of proof is on the CA to show that it has no fault.[209]

b. Failure to Inform MII before Termination

If a CA goes out of business, but fails to inform the MII at least sixty days before doing so, the MII is mandated to impose a fine against the CA's "person directly in charge" in the range of 10,000-50,000 Yuan.[210]

c. Failure to Abide by CA Regulation

The MII will sanction the CA for the following: failing to abide by its own CPS,[211] not fulfilling the retention requirement,[212] or other illegal acts.[213] The MII will order the CA to correct the behavior and will impose a deadline.[214] If the CA fails to accomplish the correction

---

[207] ESL, *supra* note 23, art. 27; *see also* CAR *supra* note 24, art. 21.
[208] ESL, *supra* note 23, art. 28; *see also* CAR *supra* note 24, art. 17.
[209] ESL, *supra* note 23, art. 28. This is a stringent provision which may drive up the cost of CA service in China, due to the need for the CA to purchase a greater amount of insurance coverage. By comparison, other jurisdictions do not place the burden of proof on the CA to show it is blameless. *See, e.g.,* Hong Kong, *supra* note 45; U.S. E-Sign Act note 301 *infra*. Nevertheless, the author appreciates this provision because it helps to ensure that CA's in China will make a special effort to ensure the trustworthiness and integrity of their computer systems.
[210] This corresponds to a range of approx. U.S. $1240-6200. *See also* CAR, *supra* note 24, art. 23 and art. 24(2).
[211] ESL, *supra* note 23, art. 31; *see also* CAR, *supra* note 24, art. 16. These are the "business rules" which have been written and disseminated by the CA; they correspond to the Certification Practice Statement ("CPS") in the U.S. and Hong Kong; *see also* Blythe, *supra* notes 34 and 50.
[212] ESL, note 23, art. 31. Certification documents must be retained for a period of five years.
[213] *Id.* at art. 31.
[214] *Id.*

by the deadline, the MII will revoke the CA's license and will prohibit the manager in charge and other responsible persons from engaging in CA activities for a period of ten years.[215] The MII will post notice of CA's revoked license, and inform the department of commerce.[216]

3. Liability of Imposter CA

If an organization is engaged in providing CA services without a license, the MII shall order it to cease and desist.[217] The MII will confiscate any illegal gains made by the imposter CA.[218] Furthermore, the MII shall impose a fine against the imposter.[219] If there are no illegal gains or the illegal gains are less than 300,000 Yuan (approx. U.S. $3718), the fine will be in the range of 100,000-300,000 Yuan.[220] If the illegal gains exceed 300,000 Yuan, the fine will be in the range of the amount of the illegal gains, up to triple the amount of the illegal gains.[221]

a. Liability for Fraudulent Use of E-Signatures

It is a crime to forge, fraudulently use, or embezzle an e-signature of another person or entity, and persons committing these acts are subject to punishment under the criminal law.[222] Additionally, the offender may become civilly liable to persons that have incurred damages because of the offender's acts.[223]

b. Government Employees' Liability for Corruption

Staff members of the MII who fail to properly carry out their licensing and supervisory duties pertaining to CAs will be administratively punished pursuant to the law.[224] If crimes are committed, they will be subject to criminal penalties as well.[225]

K. MII Charged with Responsibility to Draft Regulations

---

[215] *Id.*
[216] *Id.*
[217] *Id.* at art. 29.
[218] *Id.*
[219] *Id.*
[220] *Id.* This corresponds to a range of approx. U.S. $ 12,392-37,176.
[221] *Id.* at art. 29.
[222] *Id.* at art. 32.
[223] *Id.*
[224] *Id.* at art. 33. More specific administrative sanctions are mentioned in the CAR, *supra* note 24, art. 38.
[225] ESL, *supra* note 23, art. 33. Government corruption is an old problem in China. It still survives, notwithstanding the very stringent punishments imposed for it—up to, and including, the death penalty! For examples of capital punishment for corruption see *China Sentences 14 Officials to Death in Graft Case*, CNN.COM, (November 9, 2000), http://edition.cnn.com/2000/ASIANOW/east/11/08/china.corruption/index.html and *Former Deputy Public Security Minister Sentenced to Death*, PEOPLE'S DAILY, (Oct. 23, 2001), http://english.people.com.cn/english / 200110/23/eng20011023_82949.html. It doesn't pay to be a public whistleblower in China, either. A local Communist party official in southern China was recently given a life sentence "after he went public with complaints that senior government officials were blocking his efforts to fight corruption." Philip P. Pan, *Chinese Whistle-Blower is Given a Life Sentence*, THE ASIAN WALL STREET JOURNAL, Nov. 11-13, 2005. For a discussion of government corruption in China, the government's response to it, and possible implications for the U.S., see Benjamin van Rooij, *China's War on Graft: Politico-Legal Campaigns Against Corruption in China and Their Similarities to the Legal Reaction to Crisis in the U.S.*, 14 PAC. RIM L. & POL'Y J. 289 (2005).

The ESL consists of broad guidelines. Implementing the ESL, however, necessitates transforming it into "concrete measures."[226] Such measures are much more specific; they consist of policies, procedures, and rules to be delegated to the appropriate personnel in order to carry out the ESL's broad guidelines. Policies, sometimes referred to as standard operating procedure, are the ordinary response of the organization to a recurring type of decision or situation. Procedures are the exact sequence of steps that the CA must carry out in order to accomplish some objective. Rules are the most specific of the three and consist of fixed orders. The policies, procedures, and rules for implementing the ESL's guidelines in reference to CAs are the Certification Authority Regulations, which this article covers next.

IV. China's Certification Authority Regulations

The Certification Authority Regulations ("CAR")[227] were adopted at the 12th Executive Meeting of the Ministry of Information Industry ("MII") on January 28, 2005,[228] were promulgated on February 8, 2005,[229] and were implemented on April 1, 2005.[230] The MII created the CAR pursuant to the ESL in order to regulate CA's and CA services.[231] It emanates from the ESL, but is more detailed. The ESL and the CAR often overlap. The ESL is relatively general, and the CAR provides more specific procedural rules. The CAR provides more specific policies, procedures and rules to regulate CAs, and it serves to complement and to reinforce the broad guidelines laid out in the ESL.[232]

A. Jurisdiction and Regulatory Agency

The CAR is applicable only to CAs and their activities occurring within the People's Republic of China.[233] The Ministry of Information Industry ("MII") regulates CAs and the services they offer.[234]

B. The Licensing of a CA Organization

One of the most important duties of the MII is to license organizations that have applied to become a CA.[235]

---

[226] ESL, *supra* note 23, art. 35.
[227] CAR, *supra* note 24.
[228] *Id.* at preface.
[229] *Id.*
[230] *Id.* at preface and art. 43.
[231] ESL, *supra* note 23 art. 35; and CAR, *supra* note 24, art. 1.
[232] ESL, *supra* note 23, art. 35.
[233] Neither ESL, *supra* note 23 and CAR, *supra* note 24 do not apply in Hong Kong or in Macau; those former British and Portuguese colonies, respectively, have each been designated a "Special Autonomous Region." Pursuant to that status, Hong Kong has enacted its own E-commerce law—the ELECTRONIC TRANSACTIONS ORDINANCE (hereinafter "ETO"), Order No. 1 of 2000. For an article covering the E-Signature Law and CA Regulations of Hong Kong, *see* Blythe, *supra* note 50. To date, Macau has not enacted its own E-commerce law, although it could do so if it desired. In 2001, Macau did enact its own "telecom" law—the TELECOMMUNICATIONS BASIC LAW, *available at* http://www.gdtti.gov.mo/eng/laws/14_2001.htm. Furthermore, the ESL and the CAR do not apply in the so-called "renegade" province of Taiwan; it, too, has enacted its own legislation—the ELECTRONIC SIGNATURE LAW OF 2002, http://www.mantraco.com.tw/electronics%20signature%20lawe. *See* Blythe, *supra* note 46.
[234] CAR, *supra* note 24, art. 4. *See also* ESL, *supra* note 23, art. 18.

C. Seven Basic Requirements

The MII will not issue a license until it is satisfied that the applicant organization (1) is an autonomous legal entity; (2) has at least 30 employees (including technicians, operators, managers, security and customer service personnel); (3) is capitalized in the amount of at least thirty million Yuan;[236] (4) maintains an appropriate physical business site with an adequate environment; (5) possesses equipment and technology that meets or exceeds the national safety standards; (6) has been approved by the federal government's "encryption management" agency to be allowed to use passwords; and (7) has complied with any other laws or regulations that may apply.[237]

D. Initial Application and its Processing by MII

The prospective CA will submit an application package to the MII.[238] The package must contain (1) a completed application form; (2) affidavits prepared by the applicant's technical and managerial personnel, attesting to their qualifications; (3) affidavits pertaining to the amount of capital held by the applicant and the characteristics of the proposed business location; (4) the document prepared by the safety regulatory agency, attesting that the applicant's equipment and proposed business site meet the national safety standards; and (5) a confirmation from the national encryption agency that it has granted the applicant permission to use passwords.[239]

Upon receipt of an application, the MII will quickly review it to ensure that it complies with form requirements.[240] If it is not in the proper form, the MII will not accept it.[241] If the form is acceptable, the MII will next consider the substance[242] of the application. If necessary in order to verify the contents of the application, the MII may dispatch two or more inspectors to visit the applicant's proposed place of business.[243] The CAR also requires the MII to consult with the Ministry of Commerce to verify that the applicant has the status of a separate legal entity and other relevant matters.[244]

The MII must issue a decision to the applicant within 45 days of receipt of the application.[245] If the decision is negative, the MII is required to inform the applicant in writing of the reasons for denial of the application.[246] If the decision is positive, it will issue the license[247] to the applicant[248] and will provide the general public with the following information: (1) the

---

[235] CAR, *supra* note 24, art. 6-10 and 14.
[236] Thirty million Yuan is approximately 3.75 million U.S. dollars.
[237] CAR, *supra* note 24, art. 5. These are the more detailed aspects of the general requirements laid out in the ESL, *supra* note 23, art. 17.
[238] CAR, *supra* note 24, art. 6.
[239] *Id.*
[240] *Id.* at art 7.
[241] *Id.*
[242] *Id.* at art. 8. In the English translation of the CAR, substance is referred to as the "essence" of the application.
[243] *Id.*
[244] *Id.* at art. 9.
[245] *Id.* at art. 10. *See also* ESL, *supra* note 23, art. 18
[246] CAR, *supra* note 24, art. 10.
[247] In the English translation of the CAR, the license is referred to as a "Permit for Electronic Certification Services."
[248] CAR, *supra* note 24, art. 10.

name of the CA; (2) the serial number on the license; (3) the date of issuance of the license; and (4) the fact that the MII regulates CA's. The license will be valid for five years.[249] If any of the information changes during the five years after the license's issuance, the MII has a duty to inform the public of the changes in a timely manner.[250]

E. CA's Duty to Post Information

The MII requires the new CA to file a copy of its license with the administrative agency for industry and commerce.[251] Furthermore, before beginning to provide CA services, the CA must post the following information: (1) its legal name and registered agent;[252] (2) the location of its domicile and the preferred means of contacting the CA; (3) the serial number on its license; (4) the date of issuance of the license and the name of the agency—MII—that issued it; and (5) the period of validity of the license.[253] During the license period, if changes occur in the CA's name, domicile, legal agent or the amount of capital, the CA is required to post the changes on its website within five days of the changes.[254] Additionally, the CA is required to report the changes to the MII within fifteen days of the changes.[255]

F. Application for Renewal of the License

The CA must apply to the MII for a renewal of the license at least thirty days before the expiration date.[256] If the MII approves the renewal, the CA must post the new information (e.g., the new license period) on its website within five days.[257]

G. CA Services

The CAR requires the CA to disseminate its operating rules and to inform the subscriber of conditions pertinent to issuance of the certificate. Certain guarantees are made by the CA which should lead to specific outcomes. The CAR requires the CA to maintain confidentiality of information. The CAR also controls voluntary and involuntary termination of the CA's business.

1. Posting of CA's Operating Rules

Before beginning to offer its services to the public, each licensed CA must prepare a list of policies, procedures, and rules that it will generally follow when providing its services.[258]

---

[249] *Id.*

[250] *Id.*

[251] *Id.* at art. 11. *See also* ESL, *supra* note 23, art. 18(2).

[252] Apparently, this will facilitate the serving of process upon the CA if it is sued.

[253] CAR, *supra* note 24, art. 12. *See also* ESL, *supra* note 23, art. 18(3).

[254] CAR, *supra* note 24, art. 13.

[255] *Id.*

[256] *Id.* at art. 14.

[257] *Id.* This is the same posting procedure mentioned in CAR, *supra* note 24, art. 12.

[258] CAR, *supra* note 24, art. 15; *see also* ESL, *supra* note 23, art. 19. This idea originated in the United States, where the CA-generated rules statement is referred to as a "Certification Practice Statement." *See* ABA, *Digital Signature Guidelines* available at http://www.abanet.org/scitech/ec/isc/dsgfree.html. Hong Kong also uses the term "Certification Practice Statement" and has largely adopted the U.S. standards and procedures for preparation of the CPS; they may be found in the Hong Kong Code of Practice for Recognized Certification Authorities, Section 4 and Appendix 1, http://www.ogcio.gov.hk/textonly/eng/caro/esub3.htm. *See* Blythe, *supra* note 50.

They must be posted at the CA's website before it accepts subscribers,[259] and it must file a copy with the MII.[260] The CA must promptly post changes made to these practices, procedures, and rules at its website[261] and must report changes to the MII within thirty days after posting them.[262]

2. Informing the Subscriber

Before agreeing to issue a certificate to an applicant, the CA must inform the applicant of (1) any conditions placed upon the usage of the e-signature and the e-signature certificate; (2) how the fees are computed; (3) the applicant's duty to protect the private key and other confidential information, and liability incurred if the applicant fails in this duty; (4) the CA's duties and liabilities; and (5) other information as necessary.[263] To ensure that the applicant is fully aware of the duties and liabilities of both parties, the CA and the subscriber should enter a contract.[264]

3. Guaranteed Services

CAs guarantee to (1) create, issue, and manage e-signature certificates; (2) confirm the authenticity of e-signature certificates that it has issued; and (3) provide an online information search service pertaining to the current status of e-signature certificates it has issued.[265]

H. Expected Outcomes

The CAR considers the CA's services successful when the CA is able to (1) ensure the accuracy of the issued e-signature certificates during the period of their validity, (2) guarantee relying third parties that they will be kept apprised of developments pertaining to the e-signature certificates, and (3) maintain confidentiality of private information garnered during the CA's services.[266]

I. Privacy of Information

The CA will be liable to subscribers and to relying third parties for violating their right of privacy of personal information.[267] In order to maintain confidentiality, the CA should establish "well-developed confidentiality systems,"[268] adopt good "safety management and internal auditing systems,"[269] and obey the national confidentiality laws[270] and the MII regulations.[271]

J. Voluntary Termination of the CA's Business

---

[259] CAR, *supra* note 24, art. 15.
[260] *Id.*
[261] *Id.*
[262] *Id.*
[263] *Id.* at art. 21.
[264] *Id.* at art. 22.
[265] *Id.* at art. 17; *see also* ESL, *supra* note 23, art. 22.
[266] CAR, *supra* note 24, art. 18; *see also* ESL, *supra* note 23, art. 15.
[267] CAR, *supra* note 24, art. 20.
[268] *Id.* at art. 19.
[269] *Id.*
[270] *Id.* at art. 20; see also ESL, *supra* note 23, art. 15.
[271] CAR, *supra* note 24, art. 19.

If a CA decides to go out of business before the end of its period of licensure, it must notify all subscribers and reliant third parties at least 90 days before business activity ceases. The CA must inform subscribers of details pertaining to "succession of services" and other relevant matters.[272]

At least 60 days before going out of business, the CA must make an application to the MII to cancel the license. After the MII cancels the CA license, the CA must present the cancellation confirmation to the governmental department for industry and commerce to cancel its registration there.[273]

At least 60 days before going out of business, the CA must also begin to look for another CA to assume its role after it exits.[274] If it is unable to find another CA to assume its duties, then the CA must ask the MII to request some other CA to assume its duties.[275] If no other CA is willing to take over the departing CA's duties voluntarily, then the MII has the authority to compel another CA to take over the departing CA's duties.[276]

K. Revocation: Involuntary Termination

The MII may revoke the license of any CA that fails to carry out its duties properly.[277] In that case, the MII has the discretion to handle the situation as it sees fit.[278] The MII will look for another CA to take over the duties of the departing CA and, if necessary, may compel another CA to take over those duties.[279]

L. Electronic Signature Certificates

The CAR requires specific contents of Certificates, grounds for their cancellation, and means of verification of the subscriber's identity.

1. Mandatory Contents of Certificates

When issuing a certificate, the CA must ensure that it contains (1) the name of the CA company; (2) the name of the subscriber; (3) a serial number; (4) the effective date and the expiration date; (5) the e-signature verification data of the subscriber; (6) the CA's e-signature; and (7) other information that the MII may require.[280]

2. Grounds for Cancellation of Certificates

---

[272] *Id.* at art. 24(1); s*ee also* ESL, *supra* note 23, art. 23(1).
[273] CAR, *supra* note 24, art. 23; *see also* ESL, *supra* note 23, art. 23(2).
[274] CAR, *supra note* 24, art. 24(2); *see also* ESL, *supra* note 23, art. 23(2).
[275] CAR, *supra* note 24, art. 25; *see also* ESL, *supra* note 23, art. 23(3).
[276] CAR, *supra* note 24, art. 27; *see also* ESL, *supra* note 23, art. 23(3).
[277] CAR, *supra* note 24, art. 26; *see also* ESL, *supra* note 23, art 23(4).
[278] CAR, *supra* note 24, art. 26.
[279] CAR, *supra* note 24, art. 27; *see also* ESL, *supra* note 23, art. 23(3). If a CA refuses to assume the duties of another CA when so requested by the MII, it can be sanctioned. *See also* CAR, *supra* note 24, art. 39.
[280] CAR, *supra* note 24, art. 28; *see also* ESL, *supra* note 23, art. 21.

Any of the following is sufficient justification for the CA to cancel a certificate it has previously issued: (1) the subscriber requests it to be cancelled; (2) the CA learns that some of the information provided by the subscriber is false; (3) the subscriber fails to carry out his contractual obligations; (4) the security of the certificate is in doubt; or (5) other circumstances pursuant to law or regulations.[281] In each of the above situations, the CA is not required to cancel the certificate, but cancellation is within its discretion[282] The CA would probably cancel in these situations in order to avoid enhanced legal liability.[283] If the CA decides to cancel, the CA must post a notice on its website.[284]

M. Verification of Subscriber's Identification

The CA is required to verify all information pertaining to the identity of (1) an applicant for a certificate; (2) a subscriber applying for a renewal of a certificate; and (3) a subscriber applying for cancellation of a certificate.[285]

N. Government Oversight of CAs

CAs must uphold high standards of service during the period of their licensure.[286] Accordingly, the CAR mandates CAs to give training to employees to ensure they are fulfilling their duties properly.[287]

In order for the government to provide sufficient oversight, it requires the CA organization to submit timely and accurate statistical information and reports to the MII regarding its activities.[288] However, reports are not enough to provide effective oversight. Every year, the MII will conduct an on-site inspection of the CA in order to verify the information contained in the reports.[289]

In exceptional situations, the MII, acting through its subordinate departments at the provincial level, has the authority to directly supervise and to administer the affairs of a CA.[290]

O. Punishment Provisions

If a CA files fake documents, is deceptive, or gives false information to the MII pertaining to its activities, the MII shall order the CA to "make a correction."[291] Furthermore, the MII shall issue a warning to the CA, or may fine the CA in the range of 5,000 to 10,000 Yuan.[292]

---

[281] CAR, *supra* note 24, art. 29.
[282] *Id.*
[283] ESL, *supra* note 23, art. 27.
[284] CAR, *supra* note 24, art. 31. As mentioned, the CA also is required to post a notice on its website when a license is renewed; ESL, *supra* note 23, art. 18(3).
[285] CAR, *supra* note 24, art. 30. *See also* ESL, *supra* note 23, art. 20.
[286] CAR, *supra* note 24, art. 33.
[287] *Id.* at art. 35.
[288] *Id.* at art. 34.
[289] *Id.* at art. 32.
[290] *Id.* at art. 36; *see also* ESL *supra* note 23, art. 23(4). The maximum allowable duration of the supervision or the administration is not specified. *Id.*
[291] CAR, *supra* note 24, art. 37.
[292] *Id.* This range corresponds to approximately U.S. $ 620-$1240.

If a CA fails to abide by the CA regulations,[293] or fails to take over the duties of another CA after the MII asks it to do so,[294] the MII shall order it to make a correction within a time limit.[295] Furthermore, the MI will issue the CA a warning and/or fine the CA in an amount up to 10,000 Yuan.[296]

If a CA fails to maintain the high caliber of standards that it expressed in its application for the license,[297] the MII shall order the CA to "make a correction within a time limit."[298] Furthermore, the CA must pay a fine of not more than 30,000Yuan.[299] The CA Regulations are also cognizant of the possibility of corruption within the MII.[300] To discourage this behavior, the CAR mentions several possible administrative sanctions: "warning, demerit recording, major demerit recording, degradation, dismissal from post, or removal from office,"[301] according to the circumstances of each case.[302] Additionally, if an MII official commits a crime, that official will be subject to penalties pursuant to the criminal law.[303]

P. Impact of ESL on Previously Existing CAs

CAs in operation before the promulgation of the CA Regulations were given a "grace" period—until October 1, 2005—to get their license pursuant to the CA Regulations.[304] After October 1, 2005, no CA may continue to offer its services without a license.[305] CAs in operation before the promulgation of the CA Regulations that plan to terminate their services must follow the termination procedures specified in the CA Regulations.[306]

Q. Reciprocal Recognition of Validity of Foreign Certificates

China recognizes the legal validity of a certificate that a foreign CA issued in a foreign country, provided: China has concluded a reciprocal treaty with the foreign country, in which the two countries have agreed to recognize each other's certificates; and the MII has ratified the certificate pursuant to the "relevant agreement or reciprocal principles."[307] If recognized, the

---

[293] *Id.* at art. 16.
[294] *Id.* at art. 27; *see also* ESL, *supra* note 23, art. 23(3).
[295] CAR, *supra* note 24, art. 39.
[296] *Id.* Ten thousand Yuan is approximately U.S. $ 1240.
[297] *Id.* at art. 33.
[298] *Id.* at art. 40.
[299] *Id.* Thirty thousand Yuan is approximately U.S. $ 3720.
[300] *Id.* at art. 38. The CA Regulations of the Hong Kong Special Autonomous Region do not contain an anti-corruption provision; *see* Blythe, *supra* note 50. Neither do anti-corruption provisions exist in the U.S. UETA or E-Sign Acts; see, respectively: Stephen E. Blythe, *supra* note 34, AND ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT ("E-Sign") sec. 101-104, codified at § 15 U.S.C. 7001-31 (2000).
[301] CAR, *supra* note 24, art. 38; *see also* ESL, *supra* note 23, art. 33.
[302] CAR, *supra* note 24, art. 38.
[303] *Id. See also* ESL, *supra* note 23, art. 33.
[304] CAR, *supra* note 24, art. 41.
[305] *Id.*
[306] *Id.*
[307] *Id.* at art. 42. In the United States, the E-Sign Act mandates the U.S. to "Take a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions", *infra* note 310, sect. 301(a)(2)(D).

foreign-issued certificate will have "equal legal binding force" as a certificate issued within China pursuant to the CA Regulations.[308]

V. Conclusion

China is on the verge of a tremendous upsurge in e-commerce transactions. China's new e-signature law and CA Regulations are expected to play an important role in this regard and to accentuate this phenomenon.

China implemented the ESL on April 1, 2005 to provide for legal recognition of e-signatures in e-commerce transactions. The ESL gave an e-signature the same legal effect as if it were a handwritten one, or one made with a seal. This removal of the legal impediments toward electronic "signing" should facilitate the development of e-commerce in China. China recognizes all forms of e-signatures (including digital signatures), as long as they meet basic standards of reliability. If the transacting parties choose to use a digital signature, they will be employing asymmetric cryptology, public key infrastructure, and will be interacting with Certification Authorities ("CA").

China has a "compulsory" system of regulating CAs; it requires CA's to hold a license issued by the designated governmental agency, the Ministry of Information Industry ("MII"). An advantage of a compulsory system is that the government may be able to impose more stringent security and trustworthiness requirements than a voluntary system would. Accordingly, CAs in China should be able to provide a relatively high degree of security to their subscribers. Pursuant to the ESL, the MII issued its Measures for the Administration of Electronic Certification Services ("CA Regulations"). These are detailed policies, procedures, and rules applicable to CAs that became effective on April 1, 2005. The CA Regulations specify how to carry out the functions of a CA, and include requirements pertaining to the CA's self-generated set of standard operating procedures (the "CPS"). The CA and the CPS play an important role in the attaining of governmental oversight over the activities of CAs. Furthermore, the CA is legally liable to both subscribers and relying third parties, and, in litigation, the CA will have the legal burden of proof to show that it was not negligent. Therefore, while the ESL is rather liberal in recognizing the validity of several forms of e-signatures, simultaneously it has taken a rather conservative, stringent approach toward regulating CAs. In the opinion of the author, both of these are positive developments.

However, one criticism of the government's promulgating so many minute regulations of CAs is that it runs counter to a basic trend in worldwide electronic signature law—minimizing regulatory control by the government. The "minimalists" argue that digital signatures should be controlled more by market forces than by governmental ones. One of the counter-arguments to this point of view, however, is that the digital signature is not required for private e-commerce transactions in China. China does not confine transacting parties to utilizing a digital signature, leaving them free to choose another form of electronic signature and avoid altogether the rather stringent regulatory rules that govern CAs. A party "opting out" of the digital signature, though, may later regret that decision; that party would ordinarily have a less secure type of e-signature than that afforded by the digital signature.

---

[308] CAR, *supra* note 24, art. 42.

A. Recommendations

The Electronic Signatures Law and Certification Authority Regulations establish a good basic framework for the attainment of secure e-commerce transactions in China. They do not go far enough, however; improvements are needed.

The following additions should be considered:

1. The stringent controls placed on the CA minimize the likelihood that the CA will commit illegal acts. However, the greatest potential threat to the online consumer is often neither the CA nor the computer hacker—it is the online seller! The present computer laws in China do not sufficiently protect the naïve cyber-buyer from the unscrupulous cyber-seller.[309] Consumer protections are needed, such as: (a) requirements mandating the cyber-seller to promptly give a confirmation notice to the cyber-buyer regarding the details of the purchase after it has been consummated;[310] (b) a brief window of opportunity after consummating the purchase—about

---

[309] China has already written some commendable legislation pertaining to consumer rights: at the federal level, the CONSUMER PROTECTION LAW OF THE PEOPLE'S REPUBLIC OF CHINA (1993), and the PRODUCT QUALITY LAW OF THE PEOPLE'S REPUBLIC OF CHINA (1993), http://www.lawinfochina.com/dispe content.asp?db=1&id=1834. At the municipal level, the REGULATIONS OF SHANGHAI MUNICIPALITY ON CONSUMER LEGITIMATE RIGHTS AND INTERESTS PROTECTION (1994 Amended), http://www.lawinfochina.com/dispecontent.asp?db=1&id=967. Both were enacted before the emergence of E-commerce and do not sufficiently address the needs of cyber-buyers.

[310] The consumer disclosures could be paraphrased from those in the U.S. Electronic Signatures in Global and National Commerce Act ("E-Sign")

1. If the seller is already required to give information to the consumer in writing, provision of the information in electronic form is only allowed if:
   a. the buyer consents to the electronic form (and has not withdrawn consent); and
   b. prior to the consent, the consumer was informed in a "clear and conspicuous statement;"
      i. that he/she is not mandated to accept the electronic form, he/she may refuse to accept it, and he/she was informed of the right to withdraw the consent (and any penalties incurred because of withdrawal of consent);
      ii. whether the consent applies only to the particular transaction currently under consideration, or other transactions as well;
      iii. how to withdraw consent and how to electronically update contact information of the buyer;
      iv. how the buyer may obtain a paper copy of an electronic record, and the amount of fee (if any) charged for the copy; and
   c. the consumer:
      i. before consenting, was given a statement of the required computer hardware and software necessary to access the electronic records; and
      ii. consented electronically, "in a manner that reasonably demonstrates" that the consumer possesses enough computer knowledge and understanding to be able to "access information in the electronic form that will be used to provide the information that is the subject of the consent;" and
   d. after consent has been given, if a change in the hardware or software required to access electronic records leads to a "material risk" that the consumer won't be able to obtain access in the future, or to retain an electronic document in the future, then the seller must:
      i. provide the buyer a statement of the revised hardware and software requirements, with notice that the buyer may now withdraw the consent previously given without imposition of a fee or a penalty; and
      ii. again comply with (c), above.
2. These provisions do not affect or replace any other disclosures to the consumer which may be required under another statute, regulation or rule of law.

seven days—within which a cyber buyer should be able to change her mind and back out of the order; (c) controls are needed over cyber-sellers' telephone calls to cyber-buyers; (d) rules for a cyber-seller who runs out of stock, but is already committed to supplying a good to a cyber-buyer; (e) prohibitions of misleading, deceptive or fraudulent advertising by a cyber-seller; and (f) rules pertaining to cyber-sellers who maintain a database of consumers' private information without their consent. Iran's e-commerce consumer protections are useful as a model for items (b) through (f).[311]

2. A comprehensive computer crimes statute needs to be enacted. The statute should include the following crimes: (a) Unauthorized Access to Computer Material, (b) Unauthorized Tampering with Computer Information, (c) Unauthorized Use of a Computer Service, (d) Unauthorized Interference in the Operation of a Computer, and (e) Unauthorized Dissemination of Computer Access Codes or Passwords. The Singapore Computer Misuse Act can be used as a model.[312]

3. Because of the specialized knowledge often required in adjudicating e-commerce disputes, China should establish Information Technology Courts as courts of first instance for such disputes. The I.T. Courts would be tribunals consisting of three experts. The chairperson would be an attorney versed in e-commerce law, and the other two persons would be an I.T. expert and a business management expert. The attorney would be required to hold a law degree and be a member of the bar with relevant legal experience; the I.T. person would be required to hold a graduate degree in an I.T.-related field and have experience in that field; and the business management expert would be required to hold a graduate degree in business administration and have managerial experience. The e-commerce law of the Kingdom of Nepal is a useful model.[313]

4. E-government—offering of governmental services in electronic form—needs to be implemented by making it a part of the e-commerce statutes. China should undertake planning to pinpoint the governmental departments that would reap the greatest cost savings with e-government, and allocate I.T. resources to those departments. Additionally, China needs to develop implementation schedules for e-government with specific deadlines for completion. E-government implementation would be a very worthwhile endeavor because it would increase

---

3. Withdrawal of consent in (1), above, does not affect the legal validity of electronic records provided to the buyer before the consent was withdrawn. The buyer's withdrawal of consent is effective "within a reasonable time" after receipt of the withdrawal by the seller. The buyer may elect to treat a failure of the seller to comply with (1)(d), above, as a withdrawal of consent.

E-Sign, ss 101(c)(1)(A)—(D), 101(c)(2)(A), and 101(c)(4). (Emphasis added.) The "clear and conspicuous" requirement means just what it says—this notice should be in plain view, not hidden and accessible only by clicking on an inconspicuous link which can be easily overlooked.

[311] MLEC *supra* note 37, articles 36-39, 50-53 and 58.

[312] Republic of Singapore, COMPUTER MISUSE ACT (Cap. 50A), August 30, 1993, *available at* http://agcvldb4.agc.gov. sg/non_version/cgi-bin/cgi_gettopo.pl?actno=1998-REVED-50A.

[313] Kingdom of Nepal, ELECTRONIC TRANSACTIONS ORDINANCE NO. 32 OF THE YEAR 2061 B.S. (2005 A.D.), s 60-71. The original version, in Nepalese Language, is available at http://www.nta.gov.np/cyber_law.html. An unofficial English translation was published in the *Nepal Gazette* on September 15 and is available at http://www.most.gov.np/_adm/download/materials/1119415859.pdf. An official English version was released by the Nepal Ministry of Law, Justice and Parliamentary Affairs and was published in the *Nepal Gazette* on March 18, 2005 and is available at http://www.hlcit.gov.np/pdf/englishcyberlaw.pdf. *See* Stephen E. Blythe, "On Top of the World, and 'Wired': A Critique of Nepal's E-Commerce Law," 8:1 J. HIGH TECH. L. __ (2007).

convenience for citizens, improve efficiency, and reduce government expenses. The e-commerce statutes of the Republic of South Korea[314] and Finland[315] are useful models.

B. A Final Thought

An ancient Chinese proverb states, "[a] journey of a thousand miles must begin with a single step." China's Electronic Signature Law is a good first step, but it is only that. The law needs additions, and the author anticipates them. The government of China seems to realize the importance of having progressive e-commerce law. They understand that it is one of the keys to achieving the e-commerce boom that many are predicting. Accordingly, expect the e-commerce law of China to be continually updated. The law implemented in 2005 merely marks the beginning of the journey and not the destination.

---

[314] Korean Legislation Research Institute (hereinafter "KLRI"), FRAMEWORK ACT ON ELECTRONIC COMMERCE, art. 27, published in *Statutes of the Republic of Korea,* Vol. 13, pp. 395-400 (1999). The KLRI is an independent non-profit organization funded by the government of the Republic of South Korea. The KLRI's charge is to translate all of the Korean federal statutes into English. They do an admirable job of this and the *Statutes'* twenty volumes, in loose-leaf form, are continually updated. This is one of the Korean government's globalization thrusts. Of course, the "official" statutes are the ones in Korean Language as originally enacted. However, given that the KLRI's work is financed by the Korean government, the English-Language versions of the *Statutes* used in research for this article could be described as "*quasi*-official." *See* Blythe, *supra* note 43.

[315] Stephen E. Blythe, "Finland's Electronic Signature Act and E-Government Act: Facilitating Security in E-Commerce and Online Public Services," 31:1 HAMLINE L. REV. ___ (2007).