E-COMMERCE SECURITY IN THE LAND OF THE PHARAOHS: REFINING EGYPT'S ELECTRONIC SIGNATURE LAW

Stephen E. Blythe[1]

I. INTRODUCTION

Egypt's Electronic Signature Law (ESL), enacted in 2004, created the Information Technology Industry Development Authority (ITIDA) to implement, license, and oversee the certification authorities (CA). Under the law, a secure electronic signature attached to an electronic document may comply with statutory signature, writing, and evidentiary admissibility requirements. Licensed CAs issue certificates to verify that the holder of a private key is the party named in the certificate. The ESL is a commendable first step in creating a legal framework for e-commerce law, but this framework can be improved with certain additions.

This Article introduces the reader to Egypt, its economy, and the role of e-commerce in its economic development. Second, this Article discusses the basic aspects of electronic signatures and public key infrastructure technology, as well as the role of certification authorities. This Article also describes and evaluates the electronic signature law of Egypt. Finally, it makes recommendations to improve Egypt's electronic signature law.

II. EGYPT, ITS ECONOMY, AND ITS E-COMMERCE

Egypt became a unified kingdom around 3200 B.C. giving rise to one of the greatest civilizations in world history during the next three millennia. In 341 B.C., the Persians conquered the last native dynasty. Later, Egypt was successively controlled by the Greeks, Romans, Byzantines, Arabs, Mamluks, the Ottoman Turks, and finally the British. Egypt gained partial

---

1. Stephen E. Blythe, Professor of Business Law and Accounting, College of Business Administration, Abu Dhabi University, Abu Dhabi, United Arab Emirates. E-mail: itlawforever@aol.com. Ph.D. (Info. Tech. Law), University of Hong Kong (China), 2010; LL.M. (Info. Tech. Law) *with distinction*, University of Strathclyde (Scotland, U.K.), 2005; LL.M. (Int'l Bus. Law) University of Houston, 1992; J.D. *cum laude*, Texas Southern University, 1986; Ph.D. (Business Administration), University of Arkansas, 1979; M.B.A., Arkansas State University, 1975. Attorney at Law, Texas and Oklahoma; Certified Public Accountant, Texas. Blythe practiced solo (employment discrimination litigation) in Houston, Texas, was affiliated with the Cheek Law Firm (insurance defense litigation) in Oklahoma City, OK and was a management consultant for the city of Haikou, China. Additionally, he has taught law, accounting, management, economics, and international business at fourteen universities in the United States, Africa, and the Middle East.

independence from Britain in 1922. Full independence followed in 1952.[2]

A period of confrontation with Israel ensued over the next three decades. President Anwar Sadat launched a war with Israel in 1973. That war was unsuccessful, and Israel gained control of the Sinai Peninsula. Later, in an about-face, Sadat visited Israel, leading to the successful Camp David peace talks and a peace treaty with Israel in 1979, which restored the Sinai Peninsula to Egypt. Islamic extremists assassinated Sadat in 1981. His replacement, Hosni Mubarak, was President of Egypt until he was forced out of office due to a popular revolt in early 2011.[3]

During the administration of President Nasser from 1956 to 1970, Egypt's economy utilized centralized planning. However, since 1970 the economy has become much more open and marked by free market characteristics. Nevertheless, Egypt has been plagued with high unemployment and insufficient economic growth during much of the past four decades. From 2001 to 2003, foreign direct investment was stagnant and the annual growth rate of the gross domestic product (GDP) was only two to three percent. The Egyptian currency was allowed to float in 2003, which led to a sharp decline in its value and an increase in inflation.

In an attempt to stimulate the economy, the government enacted sweeping economic reforms in 2005, reducing personal and corporate tax rates, customs fees, energy subsidies, and privatizing some publicly-owned businesses. Although the government's budget deficit increased, the economic reforms had dramatic positive effects, including a stock market boom, GDP growth of six percent per year since 2006, and increased foreign direct investment. One of Egypt's potential sources of future economic growth is the development of its natural gas reserves.[4]

Additionally, in terms of economic investment, "Egypt has long been the cultural and information center of the Arab world."[5] Since 1985, the government has invested in its infrastructure of both communication and information technology.[6] Although, out of a population of eighty-three

---

2. *Introduction: Egypt, The World Factbook*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/geos/eg.html (last updated Mar. 23, 2011).

3. *Background Note: Egypt*, BUREAU OF NEAR EASTERN AFFAIRS, U.S. DEP'T OF STATE (Nov. 10, 2010), http://www.state.gov/r/pa/ei/bgn/5309.htm; *Government: Egypt, The World Factbook*, CIA (2011), https://www.cia.gov/library/publications/the-world-factbook/geos/eg.html (last updated Mar. 23, 2011).

4. *Communications: Egypt, The World Factbook*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/geos/eg.html (last updated Mar. 23, 2011).

5. *Background Note: Egypt, supra* note 3, at 11.

6. Sherif Kamel & Maha Hussein, *The Emergence of E-Commerce in a Developing Nation: Case of Egypt*, 9:2 BENCHMARKING: AN INTERNATIONAL JOURNAL 146, 146–53 (2002), *available at* http://www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=07E05F64F61893C0AFB15728FB88F6F3?contentType=Article&contentId=843047. For

million, only 8.62 million (slightly more than ten percent) of Egyptians are Internet users, the number of households with access to broadband continues to increase. By 2008, one million Egyptians had access to broadband Internet. Additionally, over twenty-eight percent use Internet cafes as their primary Internet access point.[7] Egypt has fifty Internet service providers and 175,000 Internet hosts.[8] Despite this growth, business-to-consumer e-commerce in Egypt has been hindered by several factors, including a preference to use cash instead of credit cards;[9] security concerns; lack of instant gratification from e-purchases; limited access to the Internet for many households; the desire for direct conversation with sellers and the opportunity to haggle over the purchase price; poorly designed, bug-infested websites; and inconsistent return policies by web sellers.[10]

Although business-to-consumer e-commerce has lagged, business-to-business e-commerce has grown steadily in Egypt.[11] One aspect of this growing e-commerce in Egypt is the cost-plus based market for electronic signatures (e-signatures). The market for e-signatures is competitive and the market size is small, resulting in a high potential growth rate for e-signatures. Consequentially, large private firms have often outsourced e-signature and public key infrastructure (PKI) services for financial and other operations.[12] Additionally, Egyptian public utilities and other government departments have adopted PKI services and e-signatures. As a result, the demand for PKI and e-signature systems in Egypt is expected to grow markedly.[13]

III. ELECTRONIC SIGNATURES

Contract law worldwide has traditionally required contracting parties

---

an analysis of Egypt's communications infrastructure, see *National Profile for the Information Society in Egypt*, U.N. ECON. & SOC. COMM. FOR W. ASIA (2005), *available at* http://www.escwa.un.org /wsis/reports/docs/Egypt_2005-E.pdf.

7. Mohamed Marwen Meddah, *Almost One Million Egyptians Have Broadband Internet Access*, STARTUPARABIA (Apr. 28, 2008), http://www.startuparabia.com/2008/04/almost-one-million-egyptians-have-broadband-internet-access/.

8. *Economy: Egypt, The World Factbook*, CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/geos/eg.html (last updated Mar. 23, 2011).

9. Ibrahim Elbeltagi, *E-Commerce and Globalization: An Exploratory Study of Egypt*, 14:3 CROSS-CULTURAL MGMT: AN INT'L J., 196, 196–201 (2007).

10. *Introduction to E-Commerce*, LINKEGYPT, http://www.linkegypt.com/blogs/b/Introduction-to-ecommerce/22/Introduction-to-ecommerce.html (last visited Apr. 2, 2011).

11. Economist Intelligence Unit, *Egypt: Overview of E-Commerce*, GLOBAL TECH. F. (Aug. 3, 2007), http://globaltechforum.eiu.com/index.asp?layout=printer_friendly&doc_id=11174.

12. See *infra* notes 28, 30–32 for a discussion of PKI and e-signatures.

13. Abdel-Hameed Nawar, E-Signature and the Digital Economy in Egypt (Aug. 28, 2006) (Working Paper), *available at* http://ssrn.com/abstract=926584.

to affix their signatures to a document.[14] With the onset of the electronic age, the e-signature made its appearance. The e-signature has been defined as "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."[15] Alternatively, e-signatures have been described as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."[16] An e-signature may take a number of forms, like a digital signature, a digitized fingerprint, a retinal scan, a pin number, a digitized image of a handwritten signature that is attached to an electronic message, or merely a name typed at the end of an e-mail message.[17]

A. Online Contracts: Four Levels of Security

When entering into a contract online, four degrees of security are possible. The first level of security merely requires a party to click an "I Agree" button on a computer screen in order to accept the offer.[18] The second level of security is invoked through the use of a password or credit card number to verify a party's intention to purchase goods or services.[19] The third level requires the use of biometrics. Biometric methods involve a unique physical attribute of the contracting party. These are inherently extremely difficult to replicate by a would-be cyber thief. Examples include a voice pattern, facial recognition, a scan of the retina or the iris, a digital reproduction of a fingerprint,[20] or a digitized image of a handwritten signature that is attached to an electronic message. In all of these, a sample is taken from the person in advance and is stored for later comparison with a person purporting to have the same identity.[21] For example, if a person's

---

14. *See*, e.g., U.C.C. §§ 2-201, 209 (2011).

15. Thomas J. Smedinghoff, *Electronic Contracts: An Overview of Law and Legislation*, 564 P.L.I. PAT 125, 162 (1999).

16. Directive 1999/93/EC, of the European Parliament and of the Council of 13 Dec. 1999 on a Community Framework for Electronic Signatures, art. 2, 2000 O.J. No (L 13) 12 (EU). The directive is covered in detail *infra* Part IV.

17. David K.Y. Tang, *Electronic Commerce: American and International Proposals for Legal Structure, in* REGULATION AND DEREGULATION: POLICY AND PRACTICE IN THE UTILITIES AND FINANCIAL SERVICES INDUSTRIES 333 (Christopher McCrudden ed., 1999).

18. Jonathan E. Stern, Note, *Federal Legislation: The Electronic Signatures in Global and National Commerce Act*, 16 BERKELEY TECH. L. J. 391, 395 (2001).

19. *Id.*

20. With the highly successful Hong Kong identity card, two thumb prints are used as a biometric identifier. *See* Rina C.Y. Chung, *Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11th America*, 4 ASIAN-PAC. L. & POL'Y J. 442, 446, 459 (2003).

21. Stern, *supra* note 18, at 395–96; *The Legality of Electronic Signatures Using Cyber-Sign is Well Established*, CYBER-SIGN, http://replay.web.archive.org/20060428170844/http://www.cybersign.com/news_news.htm (last visited April 21, 2011).

handwriting is the biometric identifier, the "shape, speed, stroke order, off-tablet motion, pen pressure and timing information" during signing is recorded. This information is almost impossible for an imposter to duplicate.[22]

The fourth level of security utilizes digital signatures. The digital signature is considered the ultimate level of security because it is more complex and provides more security than biometrics. Many laypersons erroneously assume that the digital signature is merely a digitized version of a handwritten signature. This is not the case; the digital signature refers to the entire document.[23] It is "the sequence of bits that is created by running an electronic message through a one-way hash function and then encrypting the resulting message digest with the sender's private key."[24] A digital signature has two major advantages over other forms of electronic signatures. First, it verifies authenticity that the communication came from a designated sender. Second, it verifies the integrity of the content of the message, giving the recipient assurance that the message was not altered.[25]

Digital signatures have at least two advantages over biometrics as a form of electronic signature. First, for biometrics, the attachment of a person's biological traits to a document does not ensure that the document has not been altered. That is, it "does not freeze the contents of the document."[26] Second, the recipient of the document must have a database of biological traits of all signatories dealt with in order to verify that a particular person sent the document.[27] The digital signature does not have these two weaknesses. Most seem to view the digital signature as preferable to biometric identifiers.[28] Many also recommend the use of both

---

22. *Id.*

23. The Hong Kong e-commerce law is typical in that it defines a digital signature as:

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

Electronic Transactions Ordinance, No. 1, (2000) 553 O.H.K., § 2, *available at* http://www.hklii.org/hk/legis/en/ord/553/.

24. Smedinghoff, *supra* note 15, at 146.

25. Christopher T. Poggi, *Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation*, 41 VA J. INT'L L. 224, 250–51 (2000).

26. K.H. Pun, Lucas Hui, K.P. Chow, W.W. Tsang, C.F. Chong & H.W. Chan, *Review of the Electronic Transactions Ordinance: Can the Personal Identification Number Replace the Digital Signature?*, 32 H.K. L. J. 241, 256 (2002).

27. *Id.* at 257.

28. *Id.* However, one expert in computer law and technology, Benjamin Wright, is a notable exception. Wright contends that biometrics is a preferable authentication method in the case of the general public. He concedes that digital signatures using PKI are preferable

methods. The Hong Kong government took the course of using both methods in designing its identity card.[29]

B. Digital Signature Technology: Public Key Infrastructure

The technology used with digital signatures is public key infrastructure (PKI).[30] PKI consists of four steps:

1. The first step in utilizing PKI is to create a public-private key pair. The private key will be kept in confidence by the sender, but the public key will be available online.

2. The second step is for the sender to digitally sign the message by creating a unique digest of the message and encrypting it. A hash value is created by applying a hash function—a standard mathematical function—to the contents of the electronic document. The hash value, ordinarily consisting of a sequence of 160 bits, is a digest of the document's contents. Once processed, the hash function is encrypted, or scrambled, by the signatory using his private key. The encrypted hash function is the digital signature for the document.[31]

3. Once encrypted, the sender attaches the digital signature to the message and sends both to the recipient.

4. Finally, the recipient decrypts the digital signature by using the sender's public key. If decryption is possible, the recipient knows the message is authentic, that it came from the purported sender. Finally, the recipient will create "a second message digest of the communication and compare it to the decrypted message digest. If they match, the recipient knows the message has not been altered."[32]

IV. THREE GENERATIONS OF ELECTRONIC SIGNATURE LAW

A. The First Wave: Technological Exclusivity

In 1995, Utah became the first jurisdiction in the world to enact an

---

for complex financial deals carried out by sophisticated persons. In PKI, control of the person's "private key" becomes all -important. The person must protect the private key; all of the eggs are placed in that basket, and the person carries a great deal of responsibility and risk. With biometric methods, the member of the general public shares the risk with other parties involved in the transaction, and the need to protect the private key is not so compelling. *See* Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures*, 32 UWLA L. REV. 215, 225–26 (2001).

29. Chung, *supra* note 20, at 482.

30. Susanna Frederick Fischer, *California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation*, 7 B. U. J. SCI. & TECH. L. 229, 233 (2001).

31. Pun et. al., *supra* note 26, at 249.

32. Jochen Zaremba, *International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers*, 18 CONN. J. INT'L L. 479, 512 (2003).

electronic signature law.[33] The Utah statute recognized digital signatures but not other types of electronic signatures.[34] The authors of the Utah statute believed, with some justification, that digital signatures provide the greatest degree of security for e-transactions. Utah was not alone in this belief; other jurisdictions grant exclusive recognition to the digital signature, including Argentina,[35] Bangladesh,[36] India,[37] Malaysia,[38] Nepal,[39] New Zealand,[40] and Russia.[41]

Unfortunately, these jurisdictions' decisions to allow only one form of technology are burdensome and overly restrictive. Forcing users to employ digital signatures provides greater security, but this benefit may be outweighed by the digital signature's possible disadvantages. Digital signatures are more expensive than other types of e-signatures because of the fee paid to the certification authority. Digital signatures are less convenient because the use of a certification authority is required. Additionally, users are forced to use one type of technology to the exclusion of others when another type of technology might be better suited to a particular type of transaction. They are also forced to use a more complicated technology that may be less adaptable to technologies used in

---

33. UTAH CODE ANN. §§ 46-3-101 to -602 (West 1995) *repealed by* 2006 Utah Laws 21 (2006) codified as amended at UTAH CODE ANN. §§ 46-4-101 to -503 (West 2011).

34. *Id.*

35. Digital Signature Decree, Law No. 2628/02, Dec. 19, 2002, B.O. 20/12/2002 (Arg.), *available at* http://infoleg.mecon.gov.ar/infoleginternet/anexos/80000-84999/80733/norma.htm, *amended by* Law No. 724/06, June 8, 2006, B.O. 13/06/06, *available at* http://infoleg.mecon.gov.ar/infolegIntenet/anexos/115000-119999/116998/norma.htm. *See generally* Stephen E. Blythe, *A Critique of Argentine E-Commerce Law and Recommendations for Improvement*, GOLDEN GATE U. SCH. L. ANN. SURV. INT'L & COMP. L. (forthcoming 2011).

36. LAW COMM'N OF BANGL., FINAL REPORT ON THE LAW OF INFORMATION TECHNOLOGY (2000) *available at* http://www.lawcommissionbangladesh.org/wplit.pdf.

37. Information Technology Act, No. 21 of 2000, INDIA CODE (2000), *available at* http://www.dot.gov.in/Acts/itbill2000.pdf. *See generally* Stephen E. Blythe, *A Critique of India's Information Technology Act and Recommendations for Improvement*, 34 SYRACUSE J. INT'L L. & COM. 1 (2006).

38. Digital Signature Act (Act No. 562/1997) (Malay.) *available at* http://www.msc.com.my/cyberlaws/act_digital.asp.

39. Electronic Transactions Act, Ordinance No. 32 of 2061 B.S. [2005], 54 KATHMANDU EXTRAORDINARY ISSUE 60 (Nepal) *available at* http://www.entrec.org.np/trade/files/ The%20Electronic%20Transactions%20Ordinance%20%202005.pdf. *See generally* Stephen E. Blythe, *On Top of the World, and Wired: A Critique of Nepal's E-Commerce Law*, 8:1 J. HIGH TECH. L. (2008).

40. Electronic Transactions Act 200 (N.Z.), *available at* http://www.med.govt.nz/templates/ContentTopicSummary____9829.aspx.

41. Elektronnaya Tsifrovaya Podpis' Zakona [Electronic Digital Signature Law], Jan. 10, 2002, No. 1-FZ (Russ.). *See* Beiten Burkhart, *The Law on Digital Signatures Has Been Adopted in the Russian Federation*, OUTSOURCING-RUSSIA.COM (Feb. 7, 2002), http://www.russoft.org/docs/?doc=166; Fischer, *supra* note 30, at 234–37.

other nations or by other people within the same nation. Further, with the use of this technology, there is an inappropriate risk allocation between users if fraud occurs. Ultimately, the decision to allow only one technology creates a potential disincentive to invest in the development of alternative technologies.[42]

B. The Second Wave: Technological Neutrality

Jurisdictions in the second wave overcompensated when they reversed the first wave. They did not include any technological restrictions in their statutes. They did not insist upon the utilization of digital signatures or any other form of technology to the exclusion of other types of e-signatures. These jurisdictions have been called "permissive" because they take an 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. The United States[43] is a member of the second wave. The overriding majority of U.S. jurisdictions (forty-five states, the District of Columbia, Puerto Rico, and Virgin Islands) have enacted the Uniform Electronic Transactions Act, either in its entirety or with minor amendments; that statute is a permissive second-generation model law.[44] Australia has also enacted a second-generation statute.[45]

The permissive perspective, however, does not take into account that some types of electronic 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 electronic signatures, but neither is able to provide the degree of security provided by the digital signature.

---

42. Amelia H. Boss, *The Evolution of Commercial Law Norms: Lessons To Be Learned From Electronic Commerce*, 34 BROOK. J. INT'L L. 673, 689–90 (2009). It is debatable whether technological neutrality or technological specificity is the correct road to take. *See* Sarah E. Roland, *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).

43. For an analysis of U.S. law, *see* Stephen E. Blythe, *E-Commerce and E-Signature Law of the United States of America*, UKR. J. BUS. L. (Nov. 2008). For concise coverage of American, British, European Union, and United Nations 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*, 11 RICH. J. L. & TECH. 6 (2005) [hereinafter *Digital Signature Law*].

44. Unif. Elec. Transaction Act §§ 1–21 (2009). Washington state is the only U.S. jurisdiction that currently has a first-generation statute. The following states have third-generation statutes: Alabama, Georgia, Florida, and Ohio. *See also* Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001 (2011).

45. *Electronic Transactions Act 1999* (Cth)(Austl.), *available at* http://www.comlaw.gov.au/Details/C2007C00371. *See* Fischer, *supra* note 30, at 234–37.

C. The Third Wave: A Hybrid

Singapore was in the vanguard of the third wave. In 1998, Singapore adopted a middle-of-the-road position on the various types of electronic signatures.[46] Singapore's lawmakers were influenced by the UNCITRAL Model Law on Electronic Commerce.[47] In terms of technological neutrality, Singapore adopted a hybrid model—a preference for the digital signature in terms of greater legal presumption of reliability and security, but not to the exclusion of other forms of electronic signatures.[48] Singapore did not want to become hamstrung by tying itself to one form of technology.[49] Singaporean legislators realized that technology is continually evolving and that it would be unwise to require one form of technology to the exclusion of others.[50] The digital signature is given more respect under the Singapore statute, but it is not granted a monopoly, as it was in Utah.[51] Singapore allows employment of other types of electronic signatures.[52] This technological open mindedness is commensurate with a global perspective and allows parties to more easily consummate electronic transactions with parties from other nations.[53]

---

46. *See infra* note 53 and accompanying text.

47. Model Law on Electronic Commerce, G.A. Res. 51/162, U.N. Doc. A/51/148 (1997) [hereinafter MLEC]. *See generally Digital Signature Law*, *supra* note 43.

48. Fischer, *supra* note 30.

49. *Id.*

50. *See* Stephen E. Blythe, *Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality*, 33 OHIO N.U. L. REV. 525, 525–62 (2006) [hereinafter *Singapore Computer Law*].

51. *Id.*

52. *Id.*

53. Electronic Transactions Act (Act No. 16/2010) (Sing.), *available at* http://statutes.agc.gov.sg/non_version/cgi-bin/cgi_legdisp.pl?actno=2010-ACT-16-N&doctitle=ELECTRONIC%20TRANSACTIONS%20ACT%202010%0a&date=latest&method=part&sl=1 [hereinafter ETA]. Although the original Singapore statute of 1998 granted legal recognition to most types of electronic signatures, it made a strong suggestion to users—in two ways—that they should use the digital signature because it is more reliable and more secure than the other types of electronic signatures: (1) Digital signatures were given more respect under rules of evidence in a court of law than other forms of electronic signatures. Electronic documents signed with them carried a legal presumption of reliability and security. These presumptions were not given to other forms of electronic signatures. (2) Although all forms of electronic signatures were allowed in Singapore, its electronic signature law established comprehensive rules for the licensing and regulation of certification authorities, whose critical role is to verify the of authenticity and integrity of electronic messages affixed to electronic signatures. *See Singapore Computer Law*, *supra* note 50. The ETA was amended in 2010 pertaining to application and consent, electronic originals, time and place of dispatch and receipt, invitation to make offers, automated message systems, and e-government. Another amendment opens up the possibility of technological neutrality, for example that the ETA may eventually become applicable to other security procedures like biometrics. *Differences Between Electronic Trasnactions Act*

Recently, more and more nations have joined the third wave. These nations recognize the security advantages afforded by the digital signature and indicate a preference for the digital signature over other forms of electronic signatures.[54] They exhibit this preference by requiring a digital signature using a PKI system. They require these signatures for (1) authenticating an electronic record;[55] (2) showing that an electronic record complies with any statutory requirement that a record be in paper form;[56] and (3) indicating that an electronic signature complies with a statutory requirement that a pen-and-paper signature be affixed.[57] Nevertheless, third wave jurisdictions do not appear to be as technologically restrictive as first wave jurisdictions.

The moderate position adopted by Singapore has become the progressive trend in international e-signature law. The hybrid approach has been taken by the European Union,[58] Armenia,[59] Azerbaijan[60] Barbados,[61]

1998 and Electronic Transactions Act 2010, IDA SINGAPORE, http://www.ida.gov.sg/Policies%20and%20Regulation/20100630114202.aspx (last visited Mar. 11, 2011). However, because the attainment of technological neutrality remains to be seen, the author declines to reclassify Singapore as a member of the second wave at this point.

54. *See generally* Zaremba, *supra* note 32.

55. *Id.*

56. *Id.*

57. *Id.*

58. Directive 1999/93/ED, *supra* note 16; *see* Blythe, *Digital Signature Law*, *supra* note 43, at 8–10. For concise coverage of European Union law, *see* Stephen E. Blythe, *E-Signature Law and E-Commerce Law of the European Union and its Member States*, UKR. J. BUS. L., May 2008, at 22–26. In an assessment of the effectiveness of its E-Signature Directive in 2006, the European Commission concluded that contracting parties had been slow to use digital signatures but that "many other simpler electronic signature applications had become available." Stephen E. Blythe, *E-Signature Law and E-Commerce Law of the European Union and its Member States*, UKR. J. BUS. L., May 2008, at 10. Reasons advanced by the commission for the slow rate of adoption of digital signatures include "technical problems in the marketplace, a lack of criteria for certification and mutual recognition, a lack of interoperability at national and cross-border levels, and the existence of isolated areas where certificates were used for a single purpose." *Id.* Overall, the primary reason advanced was economic caused by a typical user's decision to eschew development of a multi-application digital signature in favor of an e-signature, which is applicable to its own industry, e.g., the banking sector. *Report on the Operation of Directive 1999/93/EC on a Community Framework for Electronic Signatures*, COM (2006) 120 final (Mar. 15, 2006), *cited in* Boss, *supra* note 42, at 695–96. Despite the less than enthusiastic reception of the digital signature in Europe and elsewhere, that rate of acceptance is expected to be given a boost felt worldwide by the United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea. G.A. Res. 63/122, U.N. Doc. A/RES/63/122 (Feb. 2, 2009). The Rotterdam Rules became effective on September 23, 2009, and recognize the legal validity of electronic bills of lading. *Id.* In order to comply with the security requirements of Article 38 of the Rotterdam Rules, it will apparently be necessary to employ a digital signature. Felix W.H. Chan, *In Search of a Global Theory of Maritime Electronic Commerce: China's Position on the Rotterdam Rules*, 40 J. MAR. L. & COM. 185 (2009). Accordingly, as in Mark Twain's rumored death, any notion that the digital signature is passé appears to have been "an exaggeration." *Comprehensive Publication List*

Bermuda,[62] Bulgaria,[63] Burma,[64] China[65] Colombia,[66] Croatia,[67] Dubai,[68]

---

of Known Interviews with Samuel Langhorne Clemens (SLC) aka Mark Twain, TWAINQUOTES.COM, *available at* http://www.twainquotes.com/interviews/interviewindex 2006b.html. The digital signature appears to have a bright future because, presently at least, it provides the epitome of security.

59. Law on Electronic Document and Electronic Signature of Dec. 14, 2004, LA-40-S (Arm.), *available at* http://www.parliament.am/law_docs/150105HO40eng.pdf. *See generally* Stephen E. Blythe, *Armenia's Electronic Document and Electronic Signature Law: Promotion of Growth in E-Commerce via Greater Cyber-Security*, ARM. L. REV. (May 2008).

60. Digital Electronic Signature Law of 2003 (Azer.) *available at* http://unpan1.un.org/intradoc/groups/public/documents/UNTC/UNPAN018111.pdf. *See generally* Stephen E. Blythe, *Azerbaijan's E-Commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region*, 1 COLUM. J. E. EUR. L. 44, 44–75 (2007).

61. Electronic Transactions Act, 1 L.R.O. 2001, (2001) (Barb.) *available at* http://www.commerce.gov.bb/Legislation/Documents/CAP%20308B.PDF. *See generally* Stephen E. Blythe, *The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute*, 16 CARIBBEAN L. REV. 1 (2006).

62. Electronic Transactions Act (Act No. 26/1999) (Berm.) *available at* http://www.bermudalaws.bm/Laws/Annual%20Laws/1999/Acts/Electronic%20Transactions %20Act%201999.pdf. *See* Fischer, *supra* note 30, at 234–37.

63. Zakon za elektronniya dokument i elektronniya podpis [Law for the Electronic Document and Electronic Signature], Apr. 6, 2001, SG. 34/6 2001 (Bulg.) *available at* http://clict.lex.bg/CLICT_files/documents/laws/LEDES.pdf. *See generally* Stephen E. Blythe, *Bulgaria's Electronic Document and Electronic Signature Law: Enhancing E-Commerce with Secure Cyber-Transactions*, 17 TRANSNAT'L L. & CONTEMP. PROBS. 361 (2008).

64. Electronic Transactions Law (Act No. 5/2004) (Myan.), available at http://ibiblio.org/obl/docs/Electronic-transactions.htm. *See generally* Stephen E. Blythe, *Rangoon Enters the Digital Age: Burma's Electronic Transactions Law as a Sign of Hope for a Troubled Nation*, 3 INT'L BUS. RES. 151 (2010), *available at* http://ccsenet.org/ journal/index.php/ibr/article/view/4725.

65. Diànzǐ qiānmíng fǎ (电子签名法) [Electronic Signature Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 29, 2004, effective Apr. 1, 2005) (China). *See generally* Stephen E. Blythe, *China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce*, 7 CHI.-KENT J. INTELL. PROP. 1 (2007); Felix W.H. Chan, *E-Commerce All at Sea: China Welcomes Digital Bills of Lading Under the Electronic Signature Law 2005*, 3 OKLA. J. L. & TECH. 31 (2006).

66. L. 527/99, agosto 18, 1999, DARIO OFICIAL [D.O.] art. 26–27 (Colom.). *See generally* Stephen E. Blythe, *Computer Law of Colombia and Peru: A Comparison with the U.S. Uniform Electronic Transactions Act*, *in* PEER-TO-PEER NETWORKS AND INTERNET POLICIES ch. 2 (D. Vergos & J. Saenz, eds., 2010).

67. Zakon o elektroničkom potpisu [Electronic Signature Act] OG 10/2002., as amended, (Croat.). *See generally* Stephen E. Blythe, *Croatia's Computer Laws: Promotion of Growth in E-Commerce via Greater Cyber-Security*, 26 EUR. J. L. & ECON. 75, 75–103 (2008).

68. Law of Electronic Transactions and Commerce No. 2/2002 of Feb. 12, 2002 (U.A.E. Emirate of Dubai), *available at* http://www.tecom.ae/law/law_2.htm. *See generally* 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*, 23 J. ECON. & ADMIN. SCI. 103 (2007).

Finland,[69] Hong Kong,[70] Hungary,[71] Iceland,[72] Iran,[73] Jamaica,[74] Japan,[75] Jordan,[76] Lithuania,[77] Pakistan,[78] Peru,[79] Slovenia,[80] South Korea,[81]

---

69. Act on Electronic Signatures No. 14/2003 (Fin.) *available at* http://www.finlex.fi/en/laki/kaannokset/2003/en20030014.pdf. *See generally* Stephen E. Blythe, *Finland's Electronic Signature Act and E-Government Act: Facilitating Security in E-Commerce and Online Public Services*, 31 HAMLINE L. REV. 443, 445–69 (2008).

70. Electronic Transactions Ordinance, (2000) Cap. 553, § 2 (H.K.) *available at* http://www.legislation.gov.hk/blis_ind.nsf/CurAllEngDoc/99A98E9A0159CC63482573090 0 2AA880?OpenDocument. *See* U.C.C. §§ 2-201, -209 (2011). In its original statute, Hong Kong only recognized digital signatures and was, therefore, a member of the first wave. However, after amendments enacted in 2004, Hong Kong joined the third wave. Electronic Transactions Amendment Ordinance, (2004) Cap. 533 (H.K.). *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).

71. ACT XXXV of 2001 On Electronic Signature (2001) (Hung.), *available at* http://www.techlawed.org. *See generally* Stephen E. Blythe, *Hungary's Electronic Signature Act: Enhancing Economic Development with Secure E-Commerce Transactions*, 16 INFO. & COMM. TECH. L. 47-71 (2007).

72. Act No. 28/2001 On Electronic Signatures (2001) (Ice.), *available at* http://eng.idnadarraduneyti.is/laws-and-regulations/nr/1179. *See generally* Stephen E. Blythe, *Cyber Law of Iceland: Providing Secure E-Commerce to a Highly Computer-Literate Nation*, 37 RUTGERS COMPUTER & TECH. L.J. (forthcoming 2011).

73. Electronic Commerce Law of 2004 (Iran). *See generally* Stephen E. Blythe, *Tehran Begins to Digitize: Iran's E-Commerce Law as a Hopeful Bridge to the World*, 18 SRI LANKA J. INT'L L. 23 (2006) *available at* http://www.cmb.ac.lk/jilnew/node/27.

74. Electronic Transactions Act, (Act No. 15/2006) (Jam.), *available at* http://www.our.org.jm/index.php?option=com_content&view=article&id=761:the-electronic-transaction-act-act-15-2006&catid=123:act&Itemid=390. *See generally* Stephen E. Blythe, *Internet Law as a Potential Catalyst for Growth of Caribbean E-Commerce: Jamaica's Statute as a Model, in* READINGS BOOK OF THE ACADEMY OF BUSINESS ADMINISTRATION GLOBAL TRENDS CONFERENCE (2009).

75. Denshi shomei oyobi ninshō gyōmu nikansuru hōritsu [Law Concerning Electronic Signature and Certification Services], Law No. 102 of 2000 (Japan). *See generally* Stephen E. Blythe, *Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access*, 10 J. INTERNET L. 20 (2006).

76. Act No. 85 of 2001 (Electronic Transactions Law) (Jordan), *available at* http://www.cbj.gov.jo/uploads/Electronic_Transactions_Law.pdf. *See generally* Stephen E. Blythe, *E-Commerce Security in the Hashemite Kingdom: Calibrating Jordan's Electronic Transactions Law, in* ELECTRONIC COMMERCE (Frank Columbus ed., forthcoming 2011).

77. Law VIII – 1822 of July 11, 2000 Elektroninio Parašo Įstatymas [Law on Electronic Signature], Valstybės žinios, July 26, 2000, no. 61-1827 (Lith.). *See generally* Stephen E. Blythe, *Lithuania's Electronic Signature Law: Providing More Security in E-Commerce Transactions*, 8 BARRY L. REV. 23 (2007).

78. Electronic Transactions Ordinance, No. 51 of 2002, THE GAZETTE OF PAKISTAN EXTRAORDINARY, Sept. 11, 2002 (Pak.) *available at* http://www.tremu.gov.pk/tremu1/workingroups/pdf/ETO%20Readable.pdf. *See generally* Stephen E. Blythe, *Pakistan Goes Digital: The Electronic Transactions Ordinance as a Facilitator of Growth for E-Commerce*, 2 J. ISLAMIC ST. PRAC. INT'L L. 5 (2006).

Taiwan,[82] Tunisia,[83] Turkey,[84] United Arab Emirates,[85] Vanuatu,[86] and in

---

79. Law 27269, Ley de Firmas y Certificados Digitales [Law Regulating Digital Signatures and Certificates] May 28, 2000 (Peru), *available at* http://natlaw.com/interam/pe/ec/st/tnpeec1.htm. *See generally* Blythe, *supra* note 66, at 20–24.

80. O ELEKTRONSKEM POSLOVANJU IN ELEKTRONSKEM PODPISU [ZEPEP] [ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURE ACT] URADNI LIST REPUBLIKE SLOVENIJE [UR.L. RS] No. 57/2000 as amended (Slovn.), *available at* http://e-uprava.gov.si/eud/e-uprava/en/ECAS-Act-in-English.pdf. *See generally* Stephen E. Blythe, *Slovenia's Electronic Commerce and Electronic Signature Act: Enhancing Economic Growth with Secure Cyber-Transactions*, 6 I.C.F.A.I. J. CYBER L. 8, 8–33 (2007).

81. Jeonjaseomyeongbeob [Digital Signature Act], Act No. 5792, Feb. 5, 1999, *amended by* Act No. 6360, Jan. 16, 2001, *amended by* Act. No. 6585, Dec. 31, 2001 (S. Kor.). *See generally* 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 HOUS. J. INT'L L. 573, 601–26 (2006).

82. Diànzǐ qiān zhāngfǎ [Electronic Signatures Act] (2001) (Taiwan), *available at* http://law.moj.gov.tw/Eng/Fnews/FnewsContent.asp?msgid=944&msgType=en&keyword. *See generally* Stephen E. Blythe, Taiwan's Electronic Signature Act: Facilitating the E-Commerce Boom with Enhanced Security address at the Sixth Annual Hawaii International Conference on Business (May 25–28, 2006).

83. Law No. 83 of 2000 (Electronic Exchanges and Electronic Commerce Law), (Tunis.) *translated in Tunisia's Electronic Exchanges and Electronic Commerce Law No. 83 of 2000,* RAMI OLWAN (last updated Nov. 10, 2008), http://www.olwan.org/attachments/168_Tunisia%20E-commerce%20Law.pdf. *See generally* Stephen E. Blythe, *Computer Law of Tunisia: Promoting Secure E-Commerce Transactions with Electronic Signatures*, 20 ARAB L. Q. 240, 247-58 (2006).

84. [Law 5070 of Jan. 23, 2004, Electronic Signature Law], [Official Gazette 25355] (Turk.), *translated in* Telecomm. Auth., *5070: Electronic Signature Law*, BILGI TEKMOLOJILERI VE ILETIŞIM KURUMU, http://www.tk.gov.tr/eng/pdf/Electronic_Signature_Law.pdf (last visited Apr. 4, 2011). *See generally* Stephen E. Blythe, *Improving Cyber-Security in Turkey via Refinement of E-Commerce Law*, 28 INT'L J. MGMT (forthcoming 2011); Stephen E. Blythe, Improving Cyber-Security in the Crossroads of Eurasia: Refining Turkey's E-Commerce Law address at the International Conference on Business Management (Mar. 28–29, 2011).

85. [Federal Law No. 1 of 2006,Electronic Commerce and Transactions], [Official Gazette 442] (U.A.E.) *available at* http://www.tra.ae/pdf/legal_references/Electronic%20Transactions %20%20Commerce%20Law_Final%20for%20May%203% 202007.pdf. *See generally* Stephen E. Blythe, *Fine-Tuning the E-Commerce Law of the United Arab Emirates: Achieving the Most Secure Cyber Transactions in the Middle East*, 1 INT'L J.BUS. & SOC. SCI. 163, 165–68 (2010); Stephen E. Blythe, The New Electronic Commerce Law of the United Arab Emirates: A Progressive Paradigm for Other Middle Eastern Nations to Emulate address at the Annual International Conference on Global Business, Dubai, U.A.E. (May 10–13, 2009).

86. Electronic Transactions Act, Act. No. 24 (2000) (Vanuatu). The e-commerce law of the Commonwealth of Bermuda was used as a model for this statute. *Vanuatu E-Commerce*, LOWTAX, http://www.lowtax.net/lowtax/html/jvaecom.html (last visited Apr.10, 2011). For a discussion of the ETA by the former prime minister of Vanuatu, who introduced the bill in Parliament, see Hon. Prime Minister Barak T. Sope Maautamate, *The E-Business Act of 2000, The International Companies (E-Commerce Amendment) Act of 2000, The Companies (E-Commerce Amendment) Act of 2000: A Plain English Explanation. See generally* Stephen E. Blythe, *South Pacific Computer Law: Promoting E-Commerce in Vanuatu and*

the proposed statute of Uganda.[87] Many other nations are either currently using the hybrid approach or are considering its adoption, including Egypt.

V. EGYPT'S ELECTRONIC SIGNATURE LAW

Egypt enacted its Electronic Signature Law (ESL)[88] in 2004. The statute is remarkable because it is one of the few in the world that does not contain exclusions.[89] The ESL created the Information Technology Industry Development Authority (ITIDA). ITDIA is a public corporation affiliated with the Ministry of Communications and Information.[90]

A. Goals

ITIDA was established to work toward the following goals: (1) promote the development and transfer of information technology (IT); (2) increase the value of exports of IT products and services; (3) encourage investment in IT firms and advise small and medium sized IT firms on how to be successful; (4) promote research and development in IT and the

---

Fighting Cyber-Crime in Tonga, 10: 1 J. S. PAC. L. (2010), *available at* http://www.paclii.org/ journals/fJSPL/vol10/2.shtml.

87. Electronic Signatures Bill, 2004 (Uganda) (draft), *available at* http://www.sipilawuganda.com/files/electronic%20signatures%20bill%202004.pdf. *See generally* Stephen E. Blythe, *The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control*, 11 J. MGMT POL'Y & PRACT. (2010), *available at* http://www.na-businesspress.com/jmppopen.html.

88. Law No. 15 of 2004 (E-Signature and Establishment of the Information Technology Industry Development Authority), *Al-Jarida Al-Rasmiyya*, Apr. 21, 2004 (Egypt), *available at* http://www.uneca.org/aisi/NICI/Documents/egypt-e-signature-law.doc.

89. Other nations without exclusions include Azerbaijan and Montenegro. *See* Digital Electronic Signature Law of 2003 (Azer.), *available at* http://unpan1.un.org/intradoc/groups/public/documents/UNTC/UNPAN018111.pdf; Electronic Signature Law of 2003, OFFICIAL GAZETTE REPUBLIC MONTENEGRO No.80/04, *available at* http://www.mipa.co.me/userfiles/file/Electronic%20Commerce%20Law.pdf. Accordingly, Egypt does not have a legal presumption against the legal validity of use of the electronic form in documents pertinent to wills and testamentary trusts, marriage and divorce, real estate deeds, contracts for the sale of real estate, or in any other type of transaction. This is commendable and should promote acceptance of the electronic form in virtually all situations. For example, the worldwide aversion to electronic wills is dissipating. In 2005, Tennessee became the first American jurisdiction to recognize the legal validity of a will that is executed with an electronic signature. *See* Chad Michael Ross, *Probate—Taylor v. Holt—The Tennessee Court of Appeals Allows a Computer Generated Signature to Validate a Testamentary Will*, 35 U. MEM. L. REV. 603 (2005).

90. Law No. 15 of 2004 (E-Signature and Establishment of the Information Technology Industry Development Authority), *Al-Jarida Al-Rasmiyya*, Apr. 21, 2004, art. 2 (Egypt), *available at* http://www.uneca.org/aisi/NICI/Documents/egypt-e-signature-law.doc. The minister of communications and information was charged with issuing the ESL's implementation regulations within six months of the date of publication of the ESL. *Id.* art. 29. The ESL was published in the *Official Gazette* (*Al-Jarida Al-Rasmiyya)* shortly after April 21, 2004 and went into effect the day after it was published. *Id.* art. 30.

implementation of the knowledge gained; and (5) regulate certification authorities, the verifiers of electronic signatures.[91]

B. Authority

ITIDA is empowered by the ESL to establish technical standards for e-signatures. In regulating these standards, ITIDA issues certification authority (CA) licenses to qualified applicants. ITIDA conduct audits of CAs and determines what services CAs are qualified to perform. ITIDA helps to settle disputes involving CAs by serving as a sounding board for customer complaints regarding CA services. ITIDA also provides technical advice pertinent to disputes between CAs, subscribers, and relying third parties.

In addition to regulating CAs and e-signature standards, the ITIDA provides technical advice to IT firms and training advice for their personnel. In its support role to IT firms, the ITIDA sponsors IT trade fairs, inside and outside of Egypt, and works with firms interested in the development of the IT industry. ITIDA also helps developers of original software and databases to protect their work through "depositing, recording, and registration."[92]

C. Revenue and Budget

The ITIDA derives its revenue from various sources. First, a one percent business tax of business firms'[93] revenues participating in the IT industry is deposited in an account, which is used for development of the IT industry. Second, fees are charged[94] for issuance and renewal of CA licenses.[95] Additionally, the federal government makes a budgetary allocation; fees are charged to third parties for services rendered by ITIDA; gifts and donations are made; loans and grants are received; and returns on investment of ITIDA funds are received.[96]

ITIDA independently develops its budget based upon rules adopted for economic authorities. It has the same fiscal year as the federal government.[97] ITIDA is required to maintain a bank account for deposit of its revenues at the Central Bank of Egypt; accounts at other banks are

91. *Id.* art. 3.
92. *Id.* art. 4.
93. The ITIDA board of directors decides which firms are to be taxed. *Id.* art. 5.
94. The amount of the license fee and the procedure governing its application are to be determined by the ITIDA board of directors. *Id.* art. 5.
95. *Id.*
96. *Id.* art. 6.
97. *Id.* art. 7.

subject to the approval of the minister of finance.[98] Any budgetary surpluses incurred are carried forward to the following fiscal year.[99] After consultation with the minister of finance, part of a budget surplus may be deposited within the state treasury.[100]

D. Board of Directors

The Prime Minister of Egypt is authorized to appoint ITIDA's board of directors.[101] The board of directors is responsible for the management of ITIDA.[102] The minister of communications and information technology serves as chairman of the board of directors and has policy jurisdiction over the entity.[103] Board membership consists of the following: (1) executive head; (2) advisor from the State Council;[104] (3) representative from the Ministry of Defense;[105] (4) representative from the Ministry of Interior;[106] (5) representative from the Ministry of Finance;[107] (6) representative from the Presidential Authority;[108] and (6) seven other persons[109] with relevant expertise.[110]

The members of the board of directors serve for a renewable term of three years.[111] The prime minister issues an executive order pertinent to the compensation of the board members.[112] The board is authorized to form committees consisting of various members assigned to work on specific tasks. Some of the duties may also be assigned to the chairperson or to the ITIDA executive head.[113]

The board of directors is charged with developing the technical rules and procedures pertinent to e-signatures and electronic commerce (e-commerce). The board of directors determines the services that ITDA is authorized to perform for third parties and the fees that should be charged for those services. In addition to determining these fees, the board must

98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.* art. 8.
102. *Id.*
103. *Id.*
104. The head of the State Council will choose the incumbent of this position. *Id.*
105. The minister of defense will choose the incumbent of this position. *Id.*
106. The minister of the interior will choose the incumbent of this position. *Id.*
107. The minister of finance will choose the incumbent of this position. *Id.*
108. The head of the Presidential Department (Diwan) will choose the incumbent of this position. *Id.*
109. The minister of information and communications will choose these seven persons. *Id.*
110. *Id.*
111. *Id.*
112. *Id.*
113. *Id.*

consider ITIDA's budgetary requests each year and approve its annual budget. A part of these budgetary considerations is drafting personnel regulations. ITIDA must adhere to these regulations as it carries out its compensation and employee evaluation functions, though ITIDA is an independent agency and not subject to the constraints imposed by the federal government. Beyond compensation, the board also drafts the essential training programs to be implemented for ITIDA employees.[114] Aside from determining the services provided by ITIDA and its budget for providing those services, the board drafts standard operating procedures to serve as corporate policy of ITIDA as it carries out its "technical, financial and administrative affairs." They also develop qualifications for issuance of CA licenses as well as a code of conduct for entities and persons participating in the IT and CA industries.

The board of directors meets at least once a month and whenever its chairperson decides to convene.[115] A quorum exists if a majority of its members are in attendance. Motions are passed by a majority of the board members' votes. If there is a tie in the voting, the chairperson is empowered to break the tie. The board is authorized to invite whoever it pleases in order to attain the specific expertise it needs for decision making, but the invitee will not have the right to vote.[116]

E. ITIDA Management

On a daily basis, ITIDA is led by its executive head.[117] The executive head represents ITIDA before the courts and in its interactions with external parties. She has general accountability to the board of directors for the management of ITIDA and for the execution of its "technical, administrative and financial activities."[118] Specifically, the executive head executes the board's decisions, carries out special tasks delegated by the board, and supervises the work of ITIDA. The executive head also prepares periodic evaluations of the authority's activities, highlighting performance failures, and developing action plans for rectifying the failures. The executive head must also engage in other duties specified in the organizational regulations,[119] such as filling in for the chairperson in her

114. *Id.* art. 9. The minister of communications and information technology will issue an executive order to implement this article. *Id.*

115. *Id.* art. 10.

116. *Id.*

117. *Id.* art. 11. The executive head will be appointed by the prime minister. The amount of the executive head's compensation will be publicized in an executive order of the prime minister "based on the recommendation of the Minister with policy jurisdiction." *Id.*

118. *Id.*

119. *Id.*

absence,[120] and reviewing and acting on "reports, statistics or information" that are received from IT firms, firms with e-commerce activities, and CAs.[121]

F. Electronic Signatures: Compliance with Signing Requirement

E-signatures have the same legal force and admissibility as traditional written signatures if they follow stringent technological requirements and are considered secure.[122] Furthermore, if a statute mandates that an ink signature must be executed on a paper document to incur a legal right in a transaction, that requirement is deemed to be met with the attachment of a secure e-signature to an electronic document.[123] To be admissible as evidence, e-signatures must (1) have only one signatory; (2) ensure the signatory has sole control over the e-signature's private key; and (3) ensure any changes to the data pertinent to the e-signature or to the document to which it is attached can be detected.[124]

G. Digital Signatures and Certification Authorities

The purpose of a certificate is to identify the holder of a private key used to create a digital signature. [125] Certificates can only be issued by licensed CAs [126] after verification of information pertinent to the prospective subscribers.[127] ITIDA licenses CAs if they meet the qualifications and have paid the license fee.[128] The number of CAs will be

120. *Id.* art. 12.

121. *Id.* art. 13. However, such reports are not required of presidential authorities, the armed forces, the minister of interior, the General Intelligence Agency, or the Administration Monitoring Authority. *Id.* art. 28.

122. *Id.* art. 14.

123. *Id.* Electronic signatures created under stringent technological standards comply with the admissibility rules expressed in the Evidence Law. *Id.* The Evidence Law requirements override the provisions of the ESL in determining the validity of e-documents and e-signatures. *Id.* art. 17.

124. *Id.* art. 18.

125. The implementation regulations of the ESL contain the types of information which must be included in the certificate. *Id.* art. 20.

126. CAs that were already in business at the time of enactment of the ESA were given six months in which to obtain a license and to comply with the other provisions of the ESA and its implementation regulations. *Id.* art. 27.

127. CAs are legally responsible for ensuring the confidentiality of all information they receive from applicants for certificates, and it must not be disclosed to third parties without the permission of the applicant. *Id.* art. 21.

128. Unlike most other countries, Egypt does not seem to want to allow an unlimited number of CAs. Instead, the ESL states that CAs are to be "selected under public competition." The amount of the fee will be determined by ITIDA's board of directors and must comply with the implementation regulations of the ESL but does not have to comply with Law No. 129/1947 on public utilities. *Id.* art. 19.

limited because they will be "selected under public competition."[129] The validity period of the license will be determined by the board and must not exceed ninety-nine years.[130] ITIDA has responsibility for the establishment of the supervisory, financial, and technical oversight necessary for the licensing process.[131]

Once licensed, CAs are not allowed to cease their activities, merge with another firm or waive their license with respect to a third party without the prior written permission of ITIDA.[132] Foreign entities may be issued a CA license. Thereafter, they may issue certificates if they have complied with all of the requirements determined by ITIDA's board of directors.[133]

H. Computer Crimes

The following crimes may be punished by imprisonment and the payment of a fine in the range of E£10,000 to 100,000:[134] (1) issuance of digital certificates by a person or entity that does not have a CA license; (2) damaging an e-signature, e-document or electronic communication medium, or engaging in fraudulent activity regarding same; (3) violation of ESL articles nineteen and twenty-one; (4) procuring access to an e-signature, e-document or electronic communication medium through deceit; or (5) tampering with or making inoperable an e-signature, e-document or electronic communication medium.[135] The identification of persons committing the above crimes will be published in two daily newspapers with wide circulation at the expense of the offender.[136] The chief administrator of the entity that violated the above crimes will incur the same penalty as the entity if it is proven that she had knowledge of the crimes or her negligence led to the crimes.[137]

---

129. *Id.*

130. *Id.*

131. *Id.*

132. *Id.* CAs who violate the licensing conditions or any of the provisions of ESL Article 19 may have their license suspended or revoked. It will not be reinstated until the causes of the violations have been rectified. Additionally, if criminal acts have been committed, the CA may be subject to criminal penalties pursuant to ESL Article 23. *Id.* art. 26.

133. *Id.* art. 22.

134. As of November 19, 2009, this corresponds to a range of approximately $1,832 to $18,320, according to http://www.XE.com. The penalty range will be doubled if there are repeat violations. Law No. 15 of 2004 (E-Signature and Establishment of the Information Technology Industry Development Authority), *Al-Jarida Al-Rasmiyya*, Apr. 21, 2004, art. 23 (Egypt), *available at* http://www.uneca.org/aisi/NICI/Documents/egypt-e-signature-law.doc. Furthermore, these offenses may result in more stringent punishments pursuant to the penalty code or other laws. *Id.*

135. *Id.*

136. *Id.*

137. *Id.* art. 24.

A less serious crime occurs if a CA fails to file a required report, statistical data, or other information to ITIDA. Such a violation is punishable with a fine in the range of E£ 5,000 to 50,000.[138] Additionally, the minister of justice, acting in conjunction with the minister of information and communications, may issue an executive order authorizing ITIDA employees to serve in the capacity of a law enforcement officer in reference to computer crimes which pertain to employees' professional responsibility.[139]

VI. RECOMMENDATIONS FOR IMPROVING EGYPT'S E-COMMERCE LAW

With the enactment of its e-signature law, Egypt has taken a commendable first step toward attaining a sound legal framework for e-commerce. However, more needs to be done before that goal is realized. First, Egypt should implement e-commerce contractual rules pertaining to automated contracts; attribution; acknowledgment of receipt; time and place a message is assumed to have been sent and received; and carriage contracts. For automated contracts, the U.S. Uniform Electronic Transactions Act offers a good model.[140] For attribution, South Korea's Electronic Commerce Act offers a good model.[141] For acknowledgement of receipt, look to Singapore's Electronic Transactions Act.[142] For time and place, use Holland's Electronic Commerce Act.[143] For carriage contracts,

---

138. *Id.* art. 23. As of November 19, 2009, this corresponds to a range of approximately U.S.D. $916 to $9,160 according to http://www.XE.com. The penalty range will be doubled if there are repeat violations. Law No. 15 of 2004 (E-Signature and Establishment of the Information Technology Industry Development Authority), *Al-Jarida Al-Rasmiyya*, Apr. 21, 2004, art. 24 (Egypt), *available at* http://www.uneca.org/aisi/NICI/Documents/egypt-e-signature-law.doc.

139. *Id.* art. 25.

140. Unif. Elec. Transaction Act, § 14 (2009).

141. Framework Act on Electronic Commerce, Act No. 5834, 1999 (S. Kor.) *available at* http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025692.pdf. The Korean Legislative Research Institute (KLRI) is an independent non-profit organization funded by the Republic of South Korea. The KLRI's charge is to translate all Korean federal statutes into English. They do an admirable job of this. 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 as originally enacted. However, given that the Korean government finances the KLRI's work, the English language versions of the statutes used in research for this article could be described as "*quasi*-official." *See* Blythe, *supra* note 71.

142. Electronic Transactions Act (Act No. 16/2010), § 13 (Sing.), *available at* http://statutes.agc.gov.sg/non_version/cgi-bin/cgi_legdisp.pl?actno=2010-ACT-16-N&doctitle=ELECTRONIC%20TRANSACTIONS%20ACT%202010%0a&date=latest&method=part&sl=1.

143. Information Society Services Act, April 14, 2004, art. 11 (Neth.). *See* Blythe, *supra* note 43.

Colombia's Electronic Trade Law has a commendable paradigm.[144]

After creating additional e-commerce contractual rules, Egypt should seek to comply with additional requirements from other jurisdictions. The Egyptian statute is less thorough than other nations' e-commerce laws, as it only mentions the statutory requirements pertaining to writing and signing. In contrast, the New Zealand statute states that the electronic form may be sufficient to meet statutory requirements for several types of requirements that are not covered in Egypt's statute. For example, in New Zealand (1) an e-signature may be used to satisfy a statutory requirement that a signature or a seal be witnessed if the e-signature is reliable given the circumstances, it identifies the witness, and it indicates the signature or seal has been witnessed; (2) an e-document may be used to satisfy a statutory requirement to store a paper document; (3) if a statute mandates that information be retained in electronic form, the electronic form chosen must be reliable and must be easily accessible for reference at a later time; (4) if a statute requires that a comparison be made with an original paper document, that mandate may be met by comparison with a digital copy of the original document if the integrity of the original paper document is maintained by the e-document; and (5) in all instances mentioned here, neither the generation of a digital copy nor transmission of information in an electronic communication shall be held to be in violation of copyright law.[145] These rules, which are pertinent to compliance with other statutory requirements, should be added to the Egyptian statute. Specifically, regarding the statutory language from other jurisdictions that Egypt should adopt, two important provisions are included in the Jordanian statute. First, Egypt should allow for the transferability of electronic notes. Second, Egypt should enable the electronic transfer of funds.[146]

A further flaw in the ESL is that it fails to include consumer protections for e-commerce buyers. As a model, Egypt can look to Tunisia for an example of a nation with good consumer protections for e-commerce buyers. All of Tunisia's e-commerce consumer protections are commendable.[147] Tunisia provides buyers with a last chance to review the order before entering into it. Buyers have a ten-day window to withdraw from the agreement after it has been made. If the goods are late or if they do not conform to the specifications, buyers are entitled to a refund.

144. L. 527/99, agosto 18, 1999, DARIO OFICIAL [D.O.] art. 26–27 (Colom.).

145. Electronic Transactions Act 2000, §§ 26–32 (N.Z.), *available at* http://www.med.govt.nz/templates/ContentTopicSummary____9829.aspx.

146. Act No. 85 of 2001 (Electronic Transactions Law) arts. 19–29 (Jordan), *available at* http://www.cbj.gov.jo/uploads/Electronic_Transactions_Law.pdf.

147. Law No. 83 of 2000 (Electronic Exchanges and Electronic Commerce Law), arts. 25–37 (Tunis.) *translated in Tunisia's Electronic Exchanges and Electronic Commerce Law No. 83 of 2000,* RAMI OLWAN, http://www.olwan.org/attachments/168_Tunisia%20E-commerce% 20Law.pdf (last updated Nov. 10, 2008).

Additionally, Tunisia has required sellers to provide buyers with a ten day trial period after the goods have been received; during this window the risk remains with the seller.[148]

Beyond these consumer protections, Egypt should expand the list of computer crimes in the ESL. The following computer crimes, with appropriate penalties, should be recognized: (1) unauthorized tampering with computer information; (2) unauthorized use of a computer service; (3) unauthorized interference in the operation of a computer; (4) unauthorized dissemination of computer access codes or passwords; and (5) injection of a virus into a computer. The Singapore Computer Misuse Act can be used as a model for such additions.[149]

In order to make these regulations stronger, e-government provisions within the ESL should be strengthened. These provisions are relatively weak because they are permissive; they should be mandatory. If financial resources are available, Egypt should purchase state-of-the-art computer information systems for their governmental departments. Over the long run, the investment should pay for itself in reduced cost of government services.[150] Additionally, as Egyptians rely more and more on the Internet, this will make government services more convenient and accessible to Egyptian citizens. Accordingly, governmental departments should begin to provide services online. Hong Kong is an excellent example of a jurisdiction that has successfully implemented e-government. In Hong Kong, a substantial number of government services may now be accessed online, including scheduling an interview for a visa or scheduling a wedding before a public official.[151]

In order to properly enforce these new regulations, Egypt should create information technology (IT) courts. Because of the specialized knowledge often required in the adjudication of e-commerce disputes, information technology courts should be established as a court of first instance for e-commerce disputes. These IT courts should be tribunals

148. South Korea is one of the few nations that may offer better consumer protections than Tunisia. South Korea has enacted a separate statute focusing exclusively on e-commerce consumer protections. *See* Consumer Protection in Electronic Commerce Act, Law No. 6687, Mar. 30, 2002 *amended by* Act No. 7315, Dec. 31, 2004, *amended by* Act No. 7344, Jan. 27, 2005 (S. Kor.). Furthermore, the CPA recently underwent a major overhaul with substantial amendments in Act No. 7487 of March 31, 2005, which became effective on April 1, 2006. For a thorough analysis of the CPA, *see* Blythe, *supra* note 71. Iran also provides good consumer protections, including a window of opportunity to withdraw from an e-transaction previously entered into. However, the window in Iran is only seven days, as opposed to Tunisia's ten days. *See* Blythe, *supra* note 63.

149. Computer Misuse Act, Cap. 50A (Aug. 30, 1993) (Sing.), *available at* http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_gettopo.pl?actno=1998-REVED-50A. *See generally* Blythe, *supra* note 47.

150. Chung, *supra* note 20.

151. *See* Blythe, *supra* note 70, at 3.

consisting of three experts. The chairperson would be an attorney versed in e-commerce law, and the other two people would be an IT 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 IT expert would be required to hold a graduate degree in an IT 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 Nepal can be used as a model.[152]

In order to give these regulations full weight, Egypt should consider the fact that many e-transactions will occur between Egyptian citizens and residents and parties outside the borders of Egypt. Thus, it would be prudent for Egypt to formally state its claim to long-arm jurisdiction against any party who is a resident or citizen of a foreign country, so long as that party has established minimum contacts with Egypt.[153] Minimum contacts will exist, for example, if a cyber seller outside Egypt makes a sale to a party living within Egypt. The ESL should be applicable to the foreign person or entity outside of Egypt because that person or firm has had an effect on Egypt through the transmission of an electronic message received in Egypt. The foreign party should not be allowed to evade the Egyptian courts' jurisdiction merely because that party is not physically present in the country. After all, e-commerce is an inherently international phenomenon, unlimited by national borders.

Beyond the need to create effective regulations is the need to promote the utilization of e-signatures among the general public and to make them cheaper and more accessible. In order to accomplish this goal, Egypt's post office should be designated as a licensed CA. Several nations have successfully experimented with this idea, including Belgium. In Belgium, a national ID card contains a computer chip, which can be activated at the post office to become an e-signature of the cardholder. The Belgian post office has also implemented a promotional campaign to educate the general public about e-signatures and their availability through the post office.[154]

---

152. Electronic Transactions Act, Ordinance No. 32 of 2061 B.S. [2005], 54 KATHMANDU EXTRAORDINARY ISSUE 60, §§ 60–71 (Nepal), *available at* http://www.entrec.org.np/trade/files/The%20Electronic%20Transactions%20Ordinance%20%202005.pdf.

153. The Republic of Tonga is an example of a nation that has claimed long-arm jurisdiction over e-commerce parties. Its statute may be used as a model. *See* Blythe, *supra* note 86, at 14.

154. Wet Houdende Vaststelling van Bepaalde Regels in Verband met het Juridisch Kader voor Elektronische Handtekeningen en Certificatiediensten [Legal Framework for Electronic Signatures and Certification Services] of July 9, 2001, MONITEUR BELGE [M.B.] [Official Gazette of Belgium], Sept. 29, 2001, 33070. This statute was supplemented by the Royal Decree Organizing the Supervision and Accreditation of Certification Service Providers Issuing Qualified Certificates. Koninklijk Besluit Houdende Organisatie van de

Finally, to increase the number of locations offering CA services throughout Egypt, the Office of Registration Agents (RA) should be created. An RA is employed by a CA and works under the authority granted in the CA's license; an RA does not need a separate license. The RA is able to operate branch locations of the CA. The RA's responsibilities should include processing applications for certificates and confirming the identification documents those applicants submit. Several nations have experimented with RAs, including Peru[155] and the Slovak Republic.[156]

VII. SUMMARY AND CONCLUSIONS

Because of its stagnant rate of economic growth, the Egyptian government implemented sweeping reforms of its economic policies in 2005, including reductions in tax rates, energy subsidies and customs fees, and the privatization of some industries previously operated by the government. Those changes seem to have paid off. Since 2006, the rate of growth in GDP has significantly increased.

Currently, only ten percent of Egyptians have Internet access, but that percentage continues to grow as the country moves toward broadband and away from the much slower dial-up connections.[157] Business-to-consumer e-commerce has lagged because of limited Internet access, a preference to use cash in business transactions, and an aversion to credit cards.[158] However, business-to-business e-commerce is flourishing.[159] Additionally, more and more bureaucratic departments are switching to e-government;[160] this should reduce the cost of government services and make them more accessible and convenient for Egyptians as the percentage of Internet penetration increases. In 2004, Egypt demonstrated significant investment into e-commerce by passing the ESL.

The ESL was a commendable first step in the creation of a legal framework for e-commerce law. This framework can be improved by

---

Controle en de Accreditatie van de Certificatiedienstverleners die Gekwalificeerde Certificaten Afleveren [Royal Decree Organizing the Supervision and Accreditation of Certification Service Providers Issuing Qualified Certificates] of Dec. 6, 2002, MONITEUR BELGE [M.B.] [Official Gazette of Belgium], Jan. 17, 2003. *See generally* Blythe, *supra* note 43.

155. Law 27269, Ley de Firmas y Certificados Digitales [Law Regulating Digital Signatures and Certificates] May 28, 2000, art. 13 (Peru), *available at* http://natlaw.com/interam/pe/ec/st/tnpeec1.htm.

156. 215/2002 (III.15) O Elektronickom Podpise a o Zmene a Doplnení Niektorých Zákonov [On Electronic Signature and on Amendment of Some Acts] art. 21 (Slovk.), *available at* http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/legislativa/1-3/215_2006en.pdf. *See generally* Blythe, *supra* note 43.

157. Meddah, *supra* note 7.

158. *Introduction to E-Commerce*, *supra* note 10.

159. *Egypt: Overview of E-Commerce*, *supra* note 11.

160. Nawar, *supra* note 13.

adding e-contract rules that recognize the electronic form as a means of compliance with virtually all types of requirements contained in other statutes. These e-contract rules relate to attribution, acknowledgement of receipt, time and place of transmission and reception, automated contracts and carriage contracts. Further, there should be additional provisions relating to transferability of electronic notes and electronic funds, consumer protections, several new computer crimes, and mandatory e-government. In order to enforce these provisions, information technology courts should be created and given explicit long-arm jurisdiction. Additionally, in order to promote access to e-commerce, Egypt's post office should be made a certification authority, and registration agents should be granted the authority to accept and process applications for certificates on behalf of a certification authority.