SA12045

A CRITIQUE OF GERMAN E-COMMERCE LAW AND RECOMMENDATIONS FOR IMPROVEMENT

Stephen E. Blythe

Abstract

Germany has been experiencing rapid growth in internet accessibility and E-commerce, but its E-commerce laws need to be improved. The nation enacted the Digital Signature Act in 1997 but it was replaced by the Electronic Signature Act ("ESA") in 2001. Pursuant to the ESA, an E-signature and an E-document may be used to comply with legal requirements for: a handwritten signature; a paper document; an original paper document; and retention of a paper document. A person desiring an E-signature must apply to a Certification Service Provider ("CSP"). Accredited CSPs are required to use the most stringent security procedures; however, accreditation of German CSPs is not compulsory. The CSP issues a private key to the signatory with a digital certificate of identification. The ESA provides a satisfactory legal foundation for German E-commerce, but it needs to be supplemented. Recommended changes and additions to German E-commerce law include: (1) enactment of a comprehensive Electronic Transactions Law which would incorporate all laws pertinent to E-commerce, including E-contract rules; (2) recognition of the validity of the electronic form in compliance with several additional requirements of other statutes, including notarization; (3) deletion of all exclusions from coverage which would open the door for E-signatures and E-documents to be used in virtually all situations; (4) addition of rules for electronic automated contracts and electronic carriage contracts; (5) more consumer protections for E-buyers; (6) establishment of Information Technology. Courts for resolution of E-commerce disputes; (7) explicit claim of long-arm jurisdiction over foreign E-commerce parties; (8) accreditation of the German Post Office as a CSP; (9) adoption of a National ID Card containing a digital signature which could be activated by a CSP; and (10) enactment of additional computer crimes, including Intentional Injection of a Virus into a Computer System.

OBJECTIVES OF THE PAPER

The objectives of this paper are to: (1) consider the recent growth of internet accessibility and E-commerce in Germany; (2) discuss the basic aspects of electronic signatures, public-key-infrastructure technology and certification authorities; (3) describe the three generations of electronic signature law; (4) explain how the European Union Directives serve as a foundation for German E-commerce law; (5) cover the first German E-commerce law, the Digital Signature Act ("DSA"), which was in force during 1997-2001; (6) analyze the DSA's replacement, the Electronic Signature Act; and (7) make recommendations for refinement and supplementation of Germany's E-commerce law.

GERMANY'S INTERNET ACCESSIBILITY AND GROWTH IN E-COMMERCE

According to the CIA, 61.9 million Germans in a population of approximately 82 million accessed the internet in 2008; this is an internet penetration rate of 75 percent, which ranks 6th in the world and 1st in Europe.[1] In 2010, Germany was home to 6.1 million registered domain names.[2] In 2009, the country had almost 23.8 million internet hosts, a world ranking of 3rd.[3] In Europe, no country has a greater degree of broadband penetration than Germany.[4] Broadband replacement of narrowband has been strong since 2007.[5] Although broadband revenue in 2007 was only $8.5 billion, by 2013 that number is expected to grow to $14 billion.[6] Germany boasts the largest economy in Europe and the fifth-largest economy in the world.[7] Because of ever-increasing access to high-speed internet, German E-commerce has begun to flourish. The rise in the number of broadband connections has made E-transactions quicker and easier to consummate.

ELECTRONIC SIGNATURES

Contract law worldwide has traditionally required the parties to affix their signatures to a document.[8] With the onset of the electronic age, the electronic signature ("E-signature)

---

[1] U.S. Central Intelligence Agency, THE WORLD FACTBOOK, "Germany," 21 July 2010, pp. 3, 13; https://www.cia.gov/library/publications/the-world-factbook/geos/countrytemplate_gm.html .
[2] "Domain Names Trend in Germany," 30 August 2010, WEBHOSTING.INFO (a Directi service), p. 1; http://www.webhosting.info/domains/country_stats/DE.
[3] Note 1 supra at 13.
[4] "Germany Broadband Overview," POINT TOPIC, 17 June 2009; http://point-topic.com/content/operatorSource/profiles2/germany-broadband-overview.htm.
[5] "An Ambitious Broadband Strategy in Germany," PYRAMID RESEARCH, 9 March 2009; http://www.pyr.com/points/item/090309.htm.
[6] Id.
[7] U.S. Department of State, Bureau of European and Eurasian Affairs, "Economy," BACKGROUND NOTE: GERMANY, 12 March 2010, p. 10; http://www.state.gov/r/pa/ei/bgn/3997.htm.
[8] See, e.g., U.S. UNIFORM COMMERCIAL CODE Sect. 2-201, 2-209 (1998).

made its appearance. It 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,"[9] or as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."[10] An electronic signature may take a number of forms: 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.[11]

The National Consumer Law Center, a well-known U.S. consumer group has stated, "Given the current state of authentication technology, it's much easier to forge or steal an e-signature than a written one."[12] This statement seems to assume that all E-signatures offer an equal degree of security. However, such an assumption would be erroneous; some electronic signatures offer more security than others. It is prudent for E-Commerce participants to use the more secure types of electronic signatures, notwithstanding their greater degree of complexity and expense.

Online Contracts: Four Levels of Security

When entering into a contract online, four degrees of security are possible.

1. The first level would exist if a party accepted an offer by merely clicking an "I Agree" button on a computer screen.[13]

2. The second level of security would be incurred if secrets were shared between the two contracting parties. This would be exemplified by the use of a password or a credit card number to verify a customer's intention that goods or services were to be purchased.[14]

3. The third level is achieved with biometrics. Biometric methods involve a unique physical attribute of the contracting party, and these are inherently extremely difficult to replicate by a would-be cyber-thief. Examples include: a

---

[9] Thomas J. Smedinghoff, "Electronic Contracts: An Overview of Law and Legislation," 564 PLI/P at 125, 162 (1999).
[10] EUROPEAN UNION DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 13 DECEMBER 1999 ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES, (1999/93/EC)—19 January 2000, OJ L OJ No L 13 p.12; http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=en.
[11] David K.Y. Tang, "Electronic Commerce: American and International Proposals for Legal Structures," in REGULATION AND DEREGULATION: POLICY AND PRACTICE IN THE UTILITIES AND FINANCIAL SERVICES INDUSTRIES 333 (Chrisopher McCrudden ed., 1999).
[12] About.com, Sign Here Please (22 June 1998); netsecurity.about.com/library/weekly/aa062298.htm, cited in Michael Dessent, "Browse-Wraps, Click-Wraps and Cyberlaw: Our Shrinking (Wrap) World," 25 T. JEFFERSON L. REV. 1, 4 (2002).
[13] Jonathan E. Stern, Note, "Federal Legislation: The Electronic Signatures in Global and National Commerce Act," 16 BERKELEY TECH. L.J. 391, 395 (2001).
[14] Id.

voice pattern, face recognition, a scan of the retina or the iris within one's eyeball, a digital reproduction of a fingerprint,[15] or a digitized image of a handwritten signature that is attached to an electronic message. In all of these examples, a sample would be taken from the person in advance and stored for later comparison with a person purporting to have the same identity.[16] For example, if a person's handwriting was being used as the biometric identifer, the "shape, speed, stroke order, off-tablet motion, pen pressure and timing information" during signing would be recorded, and this information is almost impossible to duplicate by an imposter.[17]

Biometrics, despite its potential utility as a form of electronic signature, has at least two drawbacks in comparison with the digital signature: (1) The attachment of a person's biological traits to a document does not ensure that the document has not been altered, i.e., it "does not freeze the contents of the document;"[18] and (2) 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.[19] The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers.[20] Many also recommend the use of both methods; this was the course taken by the Hong Kong government in designing its identity card.[21]

4. The digital signature is considered the fourth level because it is more complex than biometrics. Many laypersons erroneously assume that the digital signature is merely a digitized version of a handwritten signature. This is not the case, however; the digital signature refers to the entire document.[22] It is

---

[15] In the highly successful Hong Kong Identity Card, the 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-PACIFIC L. & POL'Y J. 442 (2003).
[16] Note 18 supra at 395-96; and "The Legality of Electronic Signatures Using Cyber-Sign is Well Established," CYBER-SIGN, at http://www.cybersign.com/news news.htm
[17] Id.
[18] 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 HONG KONG L.J. 241, 256 (2002).
[19] Id. at 257.
[20] Id. However, one of the experts in computer law and technology—Benjamin Wright—is a notable exception. Wright contends that biometrics is a more preferable authentication method in the case of the general public, although he concedes that digital signatures using PKI are preferable 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 one basket, and the person carries a great deal of responsibility and risk. With biometric methods, the member of the general public would be sharing the risk with other parties involved in the transaction, and the need to protect the "private key" is not so compelling. See, Benjamin Wright, "Symposium: Cyber Rights, Protection, and Markets: Article, 'Eggs in Baskets: Distributing the Risks of Electronic Signatures,'" 32 WEST L.A. L. REV. 215, 225-26 (2001).
[21] Note 20 supra.
[22] The Hong Kong E-commerce law typically defines a digital signature as follows: "an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem

"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."[23] A digital signature has two major advantages over other forms of electronic signatures: (1) it verifies authenticity that the communication came from a designated sender; and (2) it verifies the integrity of the content of the message, giving the recipient assurance that the message was not altered.[24]

Digital Signature Technology: Public Key Infrastructure

The technology used with digital signatures is known as Public Key Infrastructure, or "PKI."[25] PKI consists of four steps:

1. The first step in utilizing this technology 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. Whereupon, 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.[26]

3. The third step is to attach the digital signature to the message and to send both to the recipient.

4. The fourth step is for the recipient to decrypt the digital signature by using the sender's public key. If decryption is possible the recipient knows the message is authentic, i.e., 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.[27]

---

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." Hong Kong Special Autonomous Region, ELECTRONIC TRANSACTIONS ORDINANCE, Ord. No. 1 of 2000, s 2.

[23] Note 14 supra at 146.

[24] 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).

[25] 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, 233 (2001).

[26] Note 23 supra at 249.

Advantages of the Digital Signature

Unlike biometric and other forms of electronic signatures, the digital signature will "freeze" the contents of the document at the time of its creation. Any alterations to the document's contents will result in a different hash value. Furthermore, the encryption of the hash value with the signatory's private key "links uniquely the digital signature to the signatory, i.e., the owner of the private key." [28] Although a handwritten signature is only "signatory-specific," the digital signature is both "signatory-specific" and "document-specific." [29]

The digital signature is the only form of electronic signature which satisfies all three of the UNCITRAL evaluation factors, i.e., that an electronic signature should: (1) authorize; (2) approve; and (3) protect against fraud. [30] Authorization is achieved because the digital signature will accompany the document, which allows for confirmation of the identity of the signatory. Approval is attained via computation of the hash value of the electronic document, which freezes the contents of the document at the time of its creation, and allows for detection of any subsequent alterations. Finally, there is protection against fraud because it is extremely unlikely—virtually impossible—for anyone to determine a signatory's private key with only the public key as a starting point.[31]

Disadvantages of the Digital Signature

The digital signature has at least two drawbacks. Firstly, since the private key of each person is rather difficult to memorize, they are most often stored in computers. If the computer is not kept in a secure location, the contents of the private key may be vulnerable. This heightens the necessity of maintaining the security of the private key and protecting it from intruders. However, it should be noted that this weakness of the digital signature is also common to most other forms of electronic signatures. The password or the PIN face similar security problems. Therefore, with good security policies and procedures, this disadvantage can be minimized.[32]

The other disadvantage of the digital signature pertains to the digital certificate, which must be issued by a Certification Authority ("CA").[33] Obtaining the certificate and

---

[27] Jochen Zaremba, "International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers," 18 CONN. J. INT'L L. 479, 512 (2003).
[28] Note 23 supra at 250.
[29] Id.
[30] Note 23 supra at 243.
[31] Note 23 supra at 252.
[32] Note 23 supra at 253.
[33] Certification Authority ("CA") seems to be the most common designation of an E-signature verifier around the world. Accordingly, that term is used in the general discussion of CAs in this section of the paper. However, some nations use other designations. Most notably, European Union nations, including Germany, use the designation Certification Service Provider ("CSP"). Accordingly, CSP will be used in the subsequent sections of this paper which cover the European Union Directives and the German Electronic Signature Act.

having to interact with the CA is somewhat inconvenient and costly for the user, but over time this disadvantage should be alleviated as digital signatures become more popular, easier to use, and cheaper.[34] Because the CA plays such a vital role in the viability of the digital signature, it is essential for the user to understand exactly what the CA does.

The Critical Role of the Certification Authority

In order for PKI to realize its potential, it is crucial that the user be able to ensure the authenticity of the public key (available online) used to verify the digital signature. If Smith and Jones are attempting to consummate an online transaction, Smith needs an independent confirmation that Jones' message is actually from Jones before Smith can have faith that Jones' public key actually belongs to Jones. It is possible that an imposter could have sent Jones his public key, contending that it belongs to Smith. Accordingly, a reliable third party—the Certification Authority—must be available to register the public keys of the parties and to guarantee the accuracy of the identification of the parties.[35]

The most important job of the CA is to issue certificates which confirm basic facts about the subscriber, the subject of the digital certificate. Of course, the certificate is a digitized, computer-held record containing the most pertinent information about a transaction between two transacting parties. Typical information contained in a certificate includes the following: the name and address of the CA that issued the certificate; the name, address and other attributes of the subscriber; the subscriber's public key; and the digital signature of the CA.[36] Sufficient information will be contained in the certificate to connect a public key to the particular subscriber.[37]

In making an application to a CA for a certificate, the prospective subscriber must provide some sort of photo I.D., e.g., a passport or a driver's license. If the application is approved and the certificate is issued, the CA will issue a private key to its new subscriber which corresponds to the public key. This is done, however, without disclosing the specifics of the private key.[38] The steps in this application procedure vary somewhat from CA to CA, according to the type of certificate being offered by the CA. Ordinarily, however, once the CA has verified the genuine connection between the subscriber and the public key, the certificate will be issued.[39]

In order to indicate the authenticity of the digital certificate, the CA will sign it with her digital signature. Ordinarily, the public key corresponding to the subscriber's private key will be filed in the CA's online repository which is accessible to the general public and to third parties who have need of communication with the subscriber. Additionally, the

---

[34] Id.
[35] Tara C. Hogan, Notes and Comments—Technology, "Now That the Floodgates Have Been Opened, Why Haven't Banks Rushed Into the Certification Authority Business?," 4 N.C. BANKING INST. 417, 424-25 (2000).
[36] A. Michael Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce," 75 OR. L. REV. 49, 58 (1996).
[37] Note 40 supra at 425-426.
[38] Note 14 supra at 149.
[39] Note 14 supra at 150.

online repository contains information pertaining to digital certificates which have been revoked or suspended by the CA due to lost or expired private keys. This is an important positive aspect of PKI technology: the general public has access to the status of digital signatures, and relying third parties are kept informed, allowing them to judge whether they should place reliance on communications signed with a certain private key.[40]

One of the recurring problems for digital signature lawmakers is in trying to fairly apportion the liability for risk of computer fraud between the CA and the subscriber. Nations around the world, and the state laws of the United States, have arrived at different conclusions regarding this apportionment. The problem is compounded if each CA is required to modify its practices every time it issues a certificate pertaining to a transaction affecting another jurisdiction which happens to have dissimilar digital signature laws.[41]

A digital certificate is only as reputable as the CA who issued it. If the CA is unreliable and untrustworthy, the digital certificate is also unreliable and untrustworthy. In the final analysis, a party contracting with an unknown stranger must rely upon the CA's registration expertise and its judgment that the subscriber's identification is accurate.[42]

THREE GENERATIONS OF ELECTRONIC SIGNATURE LAW

The First Wave: Technological Exclusivity

In 1995, the U.S. State of Utah became the first jurisdiction in the world to enact an electronic signature law.[43] In the Utah statute, digital signatures were given legal recognition, but other types of electronic signatures were not.[44] 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 granting exclusive recognition to the digital signature include Bangladesh,[45] India[46], Malaysia,[47] Nepal,[48] New Zealand[49] and Russia.[50]

---

[40] Note 40 supra at 426-27.
[41] Andrew B. Berman, Note, "International Divergence: The 'Keys' To Signing on the Digital Line—The Cross-Border Recognition of Electronic Contracts and Digital Signatures," 28 SYRACUSE J. INT'L L. & COM. 125, 143-44 (2001).
[42] David Hallerman, "Will Banks Become E-commerce Authorities?," 12 BANK TECH. NEWS, June 1, 1999.
[43] UTAH CODE ANN. 46-3-101 *et seq.*, 1995. This first-generation statute was repealed in 2000 and replaced with the Uniform Electronic Transactions Act, a second-generation model law. UTAH CODE ANN. 46-4-101 *et seq.* (2000); http://le.utah.gov/~code/TITLE46/46_04.htm. *See* Note 58 infra, first citation.
[44] Id.
[45] Bangladesh, INFORMATION TECHNOLOGY (ELECTRONIC TRANSACTION) ACT ("ITA") 2000 (Draft); http://www.bangladeshgateway.org/lawit.pdf .
[46] Republic of India, THE INFORMATION TECHNOLOGY ACT ("ITA"), 9 June 2000; http://www.mit.gov.in/itbillionline/itbill2000.asp. *See* Stephen E. Blythe, "A Critique of India's Information Technology Act and Recommendations for Improvement," 34 SYRACUSE JOURNAL OF

Unfortunately, these jurisdictions' decision to allow the utilization of only one form of technology is burdensome and overly-restrictive. Forcing users to employ digital signatures gives them more security, but this benefit may be outweighed by the digital signature's possible disadvantages: more expense because of the fee paid to the certification authority; lesser convenience due to being forced to use a certification authority; forcing users 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; use of a more complicated technology which may be less adaptable to technologies used in other nations, or even by other persons within the same nation; inappropriate risk allocation between users if fraud occurs; and the potential disincentive to invest in development of alternative technologies.[51]

The Second Wave: Technological Neutrality

Jurisdictions in the Second Wave overcompensated. They did the complete reversal of the First Wave and did not include any technological restrictions whatsoever 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 electronic signatures. These jurisdictions have been called "permissive" because they take a completely open-minded, liberal perspective on electronic signatures and do not contend that any one of them is necessarily better than the others. In other words, they are "technologically neutral." Permissive jurisdictions provide legal recognition of many types of electronic signatures and do not grant a monopoly to any one of them. The United States of America[52] is a

---

INTERNATIONAL LAW AND COMMERCE 1 (2006), a publication of the College of Law, Syracuse University, Syracuse, New York USA.

[47] Republic of Malaysia, DIGITAL SIGNATURE ACT ("DSA"), 1997; http://www.mycert.org.my/bill/digisign/digi1.html .

[48] Federal Democratic Republic of Nepal, ELECTRONIC TRANSACTIONS ORDINANCE NO. 32 OF THE YEAR 2061 B.S. (2005 A.D.), s 60-71. An official English version was released by the Nepal Ministry of Law, Justice and Parliamentary Affairs and was published in the *Nepal Gazette* on 18 March 2005; 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 JOURNAL OF HIGH TECHNOLOGY LAW (2008), a publication of Suffolk University School of Law, Boston, Massachusetts USA.

[49] New Zealand, ELECTRONIC TRANSACTIONS ACT 2000; http://www.med.govt.nz/templates/MultipageDocumentPage____9779.aspx.

[50] Russian Federation, ELECTRONIC DIGITAL SIGNATURE LAW, Federal Law No. 1-FZ, 10 January 2002. *See* Note 30 supra at 234-37.

[51] Amelia H. Boss, "The Evolution of Commercial Law Norms: Lessons To Be Learned From Electronic Commerce," 34:3 BROOKLYN JOURNAL OF INTERNATIONAL LAW 673, 689-90 (2009). It is debatable as to whether technological-neutrality or technological-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).

[52] For analysis of American law, *see* "E-Commerce and E-Signature Law of the United States of America," THE UKRAINIAN JOURNAL OF BUSINESS LAW, Kiev, Ukraine, November, 2008. For concise coverage of American, British, E.U. and U.N. 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: 2 RICHMOND JOURNAL OF LAW AND TECHNOLOGY 6 (2005).

member of the second wave; the overriding majority of its jurisdictions (forty-five states, the District of Columbia, and the Territories of Puerto Rico and Virgin Islands) have enacted the Uniform Electronic Transactions Act (either in its entirety or with minor amendments), a permissive second-generation model law.[53] Australia has also enacted a second-generation statute.[54]

The disadvantage of the permissive perspective is that it does not take into account that, in fact, 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 even approach the degree of security that is provided by the digital signature.

The Third Wave: A Hybrid

Singapore was in the vanguard of the Third Wave. In 1998, this country adopted a compromise, middle-of-the-road position with respect to the various types of electronic signatures. Singapore's lawmakers were influenced by the UNCITRAL Model Law on Electronic Commerce.[55] In terms of relative degree 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. Singapore did not want to become "hamstrung" by tying itself to one form of technology. 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. The digital signature is given more respect under the Singapore statute, but it is not granted a monopoly as in Utah. Singapore allows other types of electronic signatures to be employed. This technological open-mindedness is commensurate with a global perspective and allows parties to more easily consummate electronic transactions with parties from other nations.[56]

---

[53] United States of America, National Conference of Commissioners on Uniform State Laws, UNIFORM ELECTRONIC TRANSACTIONS ACT, 7A U.L.A. 20 (Supp. 2000); http://www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/ueta99.htm. The State of Washington is the only U.S. jurisdiction presently having a first-generation statute, and these states have third-generation statutes: Alabama, Georgia, Florida and Ohio. *See also* United States of America, ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT ("E-Sign"), Public Law 106-229, 15 U.S.C. 7001, 114 Stat. 464, 30 June 2000; http://www.esignrecords.org/resources/esign.pdf.

[54] Commonwealth of Australia, ELECTRONIC TRANSACTIONS ACT 1999; http://www.austlii.edu.au/au/legis/cth/consol_act/eta1999256/. *See* Note 30 supra at 234-37.

[55] 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). *See* Stephen E. Blythe, Note 58 supra, second citation.

[56] Republic of Singapore, ELECTRONIC TRANSACTIONS ACT (Cap. 88) ("ETA"), 10 July 1998; Although granting legal recognition to most types of electronic signatures, the Singapore statute implicitly makes 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 are given more respect under rules of evidence in a court of law than other forms of electronic signatures, and electronic documents signed with them carry a legal presumption of reliability and security—these presumptions are not given to other forms of electronic signatures; and (2) although all forms of electronic signatures are allowed to be used in Singapore, its electronic signature law established comprehensive rules

In recent years, more and more nations have joined the Third Wave. They recognize the security advantages afforded by the digital signature and indicate a preference for the digital signature over other forms of electronic signatures. This preference is exhibited in several ways: (1) utilization of a digital signature using a PKI system is explicitly required for authentication of an electronic record; (2) utilization of a digital signature with PKI seems to be necessary in order for an electronic record to comply with any statutory requirement that a record be in paper form; and (3) in order for a signature in electronic form to comply with a statutory requirement that a pen-and-paper signature be affixed, it must be a digital signature created with PKI. Nevertheless, the Third Wave jurisdictions do not appear to be as technologically-restrictive as those in the First Wave. They do not compel the E-commerce participant to use only the digital signature, *in lieu* of other forms of electronic signatures, as the State of Utah did in its original statute of 1995.

The moderate position adopted by Singapore has now become the progressive trend in international electronic signature law. The hybrid approach is the one taken by the European Union's E-Signatures Directive,[57] Armenia,[58] Azerbaijan[59] Barbados,[60]

---

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. Id. *See* Stephen E. Blythe, "Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality," 33 OHIO NORTHERN UNIVERSITY LAW REVIEW 525-562 (2006).

[57] Note 15 supra; *see* Stephen E. Blythe, Note 58 supra, second citation. 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," THE UKRAINIAN JOURNAL OF BUSINESS LAW, pp. 22-26, May, 2008, Kiev, Ukraine. 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." 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." Overall, the primary reason advanced was an economic one, 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, s 5.2, COM (2006), cited in Boss, Note 57 supra 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 "shot in the arm" felt worldwide by the "United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (hereinafter "Rotterdam Rules");" http://www.unis.unvienna.org/unis/pressrels/2008/unisl125.html . The Rotterdam Rules became effective on 23 September 2009 and recognize the legal validity of electronic bills of lading. 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 JOURNAL OF MARITIME LAW AND COMMERCE 185 (2009). *See also* Manuel Alba, "Electronic Commerce Provisions in the UNCITRAL Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea," 44 TEXAS INTERNATIONAL LAW JOURNAL 387 (2009). Accordingly, *a la* Mark Twain's rumored death, any notion that the digital signature is passé appears to have been "greatly exaggerated." The digital signature appears to have a bright future because, presently at least, it is the epitome of security.

[58] Republic of Armenia, LAW ON ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE, 2002; http://www.gipi.am/?i=223 . *See* Stephen E. Blythe, "Armenia's Electronic Document and Electronic

Bermuda,[61] Bulgaria,[62] Burma,[63] China[64] Colombia,[65] Croatia,[66] Dubai,[67] Finland,[68] Hong Kong,[69] Hungary,[70] Iceland,[71] Iran,[72] Jamaica,[73] Japan,[74] Jordan,[75] Lithuania,[76]

Signature Law: Promotion of Growth in E-Commerce via Greater Cyber-Security," ARMENIAN LAW REVIEW, May, 2008, a publication of the Department of Law, American University of Armenia, Yerevan, Republic of Armenia.

[59] Republic of Azerbaijan, THE LAW OF THE AZERBAIJAN REPUBLIC ON DIGITAL ELECTRONIC SIGNATURE, 2003; http://unpan1.un.org. *See* Stephen E. Blythe, "Azerbaijan's E-Commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region," 1:1 COLUMBIA JOURNAL OF EAST EUROPEAN LAW 44-75 (2007), a publication of Columbia University School of Law, New York NY USA.

[60] Barbados, ELECTRONIC TRANSACTIONS ACT, CAP. 308B, 8 March 2001; http://www.barbadosbusiness.gov.bb/miib/Legislation/Acts/investment_acts.cfm. *See* Stephen E. Blythe, "The Barbados Electronic Transactions Act: A Comparison with the U.S. Model Statute," 16 CARIBBEAN LAW REVIEW 1 (2006), a publication of the Faculty of Law, The University of the West Indies, Barbados.

[61] Commonwealth of Bermuda, ELECTRONIC TRANSACTIONS ACT 1999 ("ETA"); http://www.bakernet.com/ecommerce/bermuda-eta.doc . *See* Note 18 supra at 234-37.

[62] Republic of Bulgaria, LAW ON ELECTRONIC DOCUMENT AND ELECTRONIC SIGNATURE ("EDL"), 2001; http://www.csd.bg/news/law/E-CommercePublE.htm. *See* Stephen E. Blythe, "Bulgaria's Electronic Document and Electronic Signature Law: Enhancing E-Commerce With Secure Cyber-Transactions," 17:2 TRANSNATIONAL LAW AND CONTEMPORARY PROBLEMS 361 (2008), a publication of the University of Iowa College of Law, Iowa City, Iowa USA.

[63] The Union of Myanmar, ELECTRONIC TRANSACTIONS LAW ("ETL"), The State Peace and Development Council Law No. 5/2004, The 12 Waxing of Kason 1366 M.E., 30 April 2004; http://ibiblio.org/obl/docs/Electronic-transactions.htm. *See* Stephen E. Blythe, "Rangoon Enters the Digital Age: Burma's Electronic Transactions Law As a Sign Of Hope For a Troubled Nation," 3:1 INTERNATIONAL BUSINESS RESEARCH __ (2010), a publication of the Canadian Center of Science and Education, Toronto, Canada; http://ccsenet.org/journal/index.php/ibr/ .

[64] People's Republic of China, Order No. 18 of the President, LAW OF THE PEOPLE'S REPUBLIC OF CHINA ON ELECTRONIC SIGNATURE, Adopted at the 11th Meeting of the Standing Committee of the Tenth National People's Congress of the People's Republic of China, Promulgated 28 August 2004, Effective 1 April 2005. The statute was translated into English by the Beijing University School of Law, Beijing, China, and is available (by subscription only) at their website: http://www.lawinfochina.com/dispecontent.asp?db=1&id=3691. *See* Stephen E. Blythe, "China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce," 7 CHICAGO-KENT JOURNAL OF INTELLECTUAL PROPERTY 1 (2007), a publication of Chicago-Kent College of Law, Illinois Institute of Technology, Chicago, Illinois USA. *See also* Felix W.H. Chan, "E-Commerce All at Sea: China Welcomes Digital Bills of Lading Under the Electronic Signature Law 2005," 3 OKLAHOMA JOURNAL OF LAW AND TECHNOLOGY 31 (2006).

[65] Republic of Colombia, LAW REGULATING DATA MESSAGES, ELECTRONIC TRADE, DIGITAL SIGNATURES AND CERTIFICATION ENTITIES ("ETL"), 13 January 1999, Official Translation No. 7 by Maria del Pilar Mejia de Restrepo; http://www.qmw.ac.uk/~t16345/colombia_en_final.htm. *See* Stephen E. Blythe, "Computer Law of Colombia and Peru: A Comparison With the U.S. Uniform Electronic Transactions Act," a book chapter in INTERNET POLICIES AND ISSUES, Frank Columbus, Editor, Nova Science Publishers, Inc., New York NY USA, 2009.

[66] Republic of Croatia, ELECTRONIC SIGNATURE ACT ("ESA"), 17 January 2002; http://www.ehrvatska.hr/sdu/en/Zakonodavstvo/RH/categoryParagraph/00/document/eSignatureActOG10_2002.pdf. *See* Stephen E. Blythe, "Croatia's Computer Laws: Promotion of Growth in E-Commerce Via Greater Cyber-Security," 26: 1 EUROPEAN JOURNAL OF LAW AND ECONOMICS 75-103 (August, 2008), a publication of Springer Netherlands Ltd., Amsterdam.

[67] Emirate of Dubai, LAW OF ELECTRONIC TRANSACTIONS AND COMMERCE NO. 2/2002 ("ETL"), 12 February 2002; http://www.tecom.ae/law/law_2.htm. *See* 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 103 (2007).

[68] Republic of Finland, Ministry of Justice, ACT ON ELECTRONIC SIGNATURES, 2003; http://www.finlex.fi. *See* Stephen E. Blythe, "Finland's Electronic Signature Act and E-Government Act: Facilitating Security in E-Commerce and Online Public Services," 31:2 HAMLINE LAW REVIEW 445-469 (2008), a publication of Hamline University School of Law, St. Paul, Minnesota USA.

[69] Hong Kong Special Autonomous Region, People's Republic of China, ELECTRONIC TRANSACTIONS ORDINANCE, Ordinance No. 1 of 2000. 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 enacted, 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 NORTH CAROLINA JOURNAL OF LAW AND TECHNOLOGY 1 (2005), a publication of the University of North Carolina School of Law, Chapel Hill, NC USA.

[70] Republic of Hungary, ACT XXXV of 2001 ON ELECTRONIC SIGNATURE, 2001; http://www.techlawed.org. *See* Stephen E. Blythe, "Hungary's Electronic Signature Act: Enhancing Economic Development With Secure E-Commerce Transactions," 16:1 INFORMATION AND COMMUNICATIONS TECHNOLOGY LAW 47-71 (2007), a publication of Routledge Publishing Co., a member of the Taylor & Francis Group. Executive Editor: Prof. Indira Carr, Centre for Legal Research, Middlesex University, London, U.K.

[71] Republic of Iceland, Ministry of Industry and Commerce, MERCHANTS AND TRADE—ACT NO. 28/2001 ON ELECTRONIC SIGNATURES, 2001; http://eng.idnadarraduneyti.is/laws-and-regulations/nr/1179. *See* Stephen E. Blythe, "Cyber Law of Iceland: Providing Secure E-Commerce to a Highly Computer-Literate Nation," 37:1 RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL ___(2012), a publication of Rutgers School of Law, Newark, New Jersey USA; http://www.rctlj.org.

[72] Islamic Republic of Iran, ELECTRONIC COMMERCE LAW OF THE ISLAMIC REPUBLIC OF IRAN ("ECL"); 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," 18 SRI LANKA JOURNAL OF INTERNATIONAL LAW (2006), a publication of the University of Colombo Faculty of Law, Colombo, Sri Lanka.

[73] Jamaica, ELECTRONIC TRANSACTIONS ACT, 2005. *See* Stephen E. Blythe, "Internet Law As A Potential Catalyst For Growth Of Caribbean E-Commerce: Jamaica's Statute As A Model," a paper presented and published in the READINGS BOOK OF THE ACADEMY OF BUSINESS ADMINISTRATION GLOBAL TRENDS CONFERENCE, Cancun, Mexico, December 19-22, 2009.

[74] Japan, LAW CONCERNING ELECTRONIC SIGNATURES AND CERTIFICATION SERVICES, promulgated 24 May 2000, effective 1 April 2001; http://www.meti.go.jp/english/report/data/gesignconte.html. *See* Stephen E. Blythe, "Cyber-Law of Japan: Promoting E-Commerce Security, Increasing Personal Information Confidentiality and Controlling Computer Access," 10 JOURNAL OF INTERNET LAW 20 (2006), a publication of Aspen Publishers, Inc., New York, NY USA.

[75] Hashemite Kingdom of Jordan, ELECTRONIC TRANSACTIONS LAW NO. 85 OF 2001; http://www.cbj.gov.jo/uploads/Electronic_Transactions_Law.pdf . *See* Stephen E. Blythe, "E-Commerce Security in the Hashemite Kingdom: Calibrating Jordan's Electronic Transactions Law," to be published in 2011 as a book chapter in ELECTRONIC COMMERCE, Frank Columbus, Editor, Nova Science Publishers, Inc., Hauppauge, New York USA. This book will become available for purchase at www.novapublishers.com.

[76] Republic of Lithuania, LAW ON ELECTRONIC SIGNATURE, No. VIII—1822 (July 11, 2000), As Amended, No. IX—934 (June 6, 2002); http://www3.lrs.lt/cgibin/preps2?Condition1=204802&Condition2. *See* Stephen E. Blythe, "Lithuania's Electronic Signature Law: Providing More Security in E-Commerce Transactions," 8 BARRY LAW REVIEW 23 (2007), a publication of Dwayne O. Andreas School of Law, Barry University, Orlando, Florida USA.

Pakistan,[77] Peru,[78] Slovenia,[79] South Korea,[80] Taiwan,[81] Tunisia,[82] United Arab Emirates,[83] Vanuatu[84] and in the proposed statute of Uganda.[85] Many other nations are currently using the hybrid approach; Germany is one of them.

---

[77] Islamic Republic of Pakistan, ELECTRONIC TRANSACTIONS ORDINANCE, 2002; http://unpan1.un.org/groups/public/documents/apcity/unpan010245.pdf. *See* Stephen E. Blythe, "Pakistan Goes Digital: the Electronic Transactions Ordinance as a Facilitator of Growth for E-commerce," 2:2 JOURNAL OF ISLAMIC STATE PRACTICES IN INTERNATIONAL LAW 5 (2006), a publication of ElectronicPublications.org Ltd., Stockport, U.K. Editors: Prof. Javaid Rehman, School of Law, Brunel University, West London, U.K.; and Dr. Amir Ali Majid, School of Law, London Metropolitan University, London, U.K.

[78] Republic of Peru, LAW REGULATING DIGITAL SIGNATURES AND CERTIFICATES, 28 May 2000, translated by National Law Center for Inter-American Free Trade; http://natlaw.com/interam/ar/ec/tn/tnarecl.htm. *See* Note 54 supra.

[79] Republic of Slovenia, Centre for Informatics, ELECTRONIC COMMERCE AND ELECTRONIC SIGNATURE ACT, 2000; http://e-uprava.gov.si/eud/e-uprava/en/ECAS-Act-in-English.pdf. *See* Stephen E. Blythe, "Slovenia's Electronic Commerce and Electronic Signature Act: Enhancing Economic Growth With Secure Cyber-Transactions," 6: 4 THE I.C.F.A.I. JOURNAL OF CYBER LAW 8-33 (2007), a publication of ICFAI University Press, Institute of Chartered Financial Analysts of India, Hyderabad, India.

[80] Korean Legislation Research Institute, DIGITAL SIGNATURE ACT NO. 5792, *Statutes of the Republic of Korea,* Vol. 16 (II), pp. 1217-1220 (1999). The statute has been amended two times: (1) Act No. 6360 of 16 January 2001; and (2) Act. No. 6585 of 31 December 2001. *See* 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 HOUSTON JOURNAL OF INTERNATIONAL LAW 573-661 (2006), a publication of the College of Law, University of Houston, Houston, Texas USA.

[81] Republic of China, ELECTRONIC SIGNATURES ACT ("ESA"), 2002; http://law.moj.gov.tw/Eng/Fnews/FnewsContent.asp?msgid=944&msgType=en&keyword. *See* 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 USA, May 25-28, 2006.

[82] Republic of Tunisia, ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE LAW, 9 August 2000; http://www.bakernet.com.org. *See* Stephen E. Blythe, "Computer Law of Tunisia: Promoting Secure E-Commerce Transactions With Electronic Signatures," 20 ARAB LAW QUARTERLY 317-344 (2006), a publication of Brill Academic Publishers, Leiden, The Netherlands.

[83] United Arab Emirates, FEDERAL LAW NO. (1) OF 2006 ON ELECTRONIC COMMERCE ANDTRANSACTIONS ("ECL"), 30 January 2006; http://www.tra.ae/pdf/legal_references/Electronic%20Transactions%20%20Commerce%20Law_Final%20for%20May%203%202007.pdf. *See* Stephen E. Blythe, "The New Electronic Commerce Law of the United Arab Emirates: A Progressive Paradigm for Other Middle Eastern Nations to Emulate," a paper presented and published in the PROCEEDINGS OF THE ANNUAL INTERNATIONAL CONFERENCE ON GLOBAL BUSINESS, Dubai, United Arab Emirates, May 10-13, 2009.

[84] Republic of Vanuatu, ELECTRONIC TRANSACTIONS ACT (Act. 24 of 2000); http://www.paclii.org/cgi-paclii/disp.pl/vu/legis/num%5fact/eta2000256.html. The E-commerce law of the Commonwealth of Bermuda was used as a model for this statute. "Vanuatu E-commerce," LOWTAX, p. 1; http://www.lowtax.net/lowtax/html/jvaecom.html. For a discussion of the ETA by the Prime Minister of Vanuatu—the person who introduced the bill in Parliament—*see* Hon. Prime Minister Barak T. Sope Maautamate, MP, Government of the Republic of Vanuatu, "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," pp. 3-7; http://www.vanuatu.gov.vu/government/library/Explanation%20of%20the%20ecommerce%20acts.htm. *See also* Stephen E. Blythe, "South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga," 10: 1 JOURNAL OF SOUTH PACIFIC LAW (2006), a publication of the School of Law, University of the South Pacific, Emalus Campus, Port Vila, Republic of Vanuatu.

THE FOUNDATON OF GERMAN E-COMMERCE LAW: THE EUROPEAN UNION DIRECTIVES

E-Signatures Directive

The European Union enacted the E-Signatures Directive (hereinafter "ESD") on 13 December 1999.[86] The purposes of the ESD are to: promote the legal recognition of E-signatures; and create a legal framework for E-signatures and certification services, resulting in their greater use.[87] However, contract law and law relating to the use of documents are not the concern of the ESD.[88] The ESD contains definitions of a(n): E-signature;[89] advanced E-signature;[90] certification service provider ("CSP");[91] and certificate.[92]

Legal Impact of E-Signatures

If a statute requires a handwritten signature affixed to a paper document, that requirement is deemed to have been met if an advanced E-signature (supported with a qualified certificate and generated with a secure signature-creation device) is attached to an E-document.[93] Furthermore, such an E-signature is admissible as evidence in a court of law.[94] An E-signature's legal recognition and admissibility as evidence may not be denied merely because of: its electronic form; lack of a qualified certificate, or the fact that the

---

[85] Republic of Uganda, ELECTRONIC SIGNATURES ACT, Draft, 2004; http://www.sipilawuganda.com/downloads/electronic%20signatures%20bill%202004.pdf. *See* Stephen E. Blythe, "The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control," a paper to be presented and published in the PROCEEDINGS OF THE TENTH ANNUAL CONFERENCE OF THE INTERNATIONAL ACADEMY OF AFRICAN BUSINESS AND DEVELOPMENT, Kampala, Uganda, May 19-23, 2009. This paper will be published as Chapter 2 in PEER-TO-PEER NETWORKS AND INTERNET POLICIES, D. Vergos and J. Saenz, Editors, © 2010 Nova Science Publishers, Inc., Hauppauge, New York USA (ISBN: 978-1-60876-287-3); to become available for purchase at www.novapublishers.com.

[86] Note 15 [?] supra.

[87] ESD art. 1.

[88] Id., ESD preamble 17.

[89] It is: "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication." ESD art. 2(1).

[90] It is an E-signature which complies with these requirements: "(a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable." ESD art. 2(2).

[91] It is: "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures." ESD art. 2(11). "Other services" include: registration services; time-stamping services; directory services; computing services; and consultancy services pertinent to E-signatures. ESD preamble 9.

[92] It is: "an electronic attestation which links signature-verification data to a person and confirms the identity of that person." ESD art. 2(9). Furthermore, a "qualified" certificate is one which meets more stringent requirements and which has been issued by a CSP with greater qualifications. ESD art. 2(10).

[93] ESD art. 5(1)(a).

[94] ESD art. 5(1)(b).

certificate was not issued by an accredited CSP; or the fact it was not generated with a secure signature-creation device.[95]

Certification Service Providers

A CSP is not mandated to hold a license,[96] and is not required to be accredited.[97] Nevertheless, each Member State must regulate all of its CSP's who issue qualified certificates.[98] These CSP's must meet more stringent qualifications than those which do not issue qualified certificates;[99] for example, they must use a secure signature-creation device[100] and must provide for secure signature verification.[101] A Member State is only allowed to regulate domestic CSP's; it is not allowed to regulate or restrict the services of a CSP established in another Member State.[102] A CSP who has issued a qualified certificate (or guaranteed a qualified certificate issued by another CSP) is legally liable for damage incurred by a relying third party who has reasonably relied on that certificate for: accuracy of information stated therein, or for completeness of information that the

[95] ESD art. 5(2). Accordingly, even a simple, non-advanced E-signature (e.g., a signed E-mail) is admissible evidence in the European Union. Martha L. Arias, "Internet Law—The EU Law on Electronic Signatures and its Recent Report, IBLS INTERNET LAW—NEWS PORTAL, 3 December 2007, p. 2; http://www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1920 .

[96] ESD art. 3(1). However, a Member State may adopt a voluntary accreditation program in order to recognize those CSP's with greater qualifications who are able to provide a higher standard of service. ESD art. 3(2). If adopted, such programs must be "objective, transparent, proportionate and non-discriminatory." Id. The number of accredited CSP's may not be limited. Id.

[97] ESD preamble 12.

[98] ESD art. 3(3). A qualified certificate must contain: designation of qualified status; name of CSP and State of creation; advanced E-signature of the CSP; name of subscriber (or pseudonym); a specific attribute of the subscriber, if essential to carry out the purpose of the certificate; a public key which corresponds to the private key; period of validity; identification number; and any limitations on purpose or value. ESD Annex I.

[99] Those qualifications are: reliability; maintenance of a secure directory and revocation service; ability to record the date and hour of issuance and revocation of a certificate; ability to confirm the identity and any special attributes of the subscriber; employ personnel with sufficient knowledge, experience and skill; possess and use trustworthy and secure computer systems and products; ability to guard against forgery of certificates and compromise of security of signature creation data; possession of sufficient financial resources and liability insurance; ability to securely store certificate-related information for the required period of time; prevention of retention or copying of signature creation data; and ability to provide written information to the subscriber before entering into a contract with him. ESD Annex II.

[100] A secure signature-creation device must utilize a technology and procedures which ensure: the data contained therein is reasonably secure and can be used only once; the data cannot be mathematically derived; the data can be protected by the subscriber from use by others; and the data will not be modified or given to the subscriber before the desired date of execution. ESD Annex III. Determination of the standards for these devices must be developed by "appropriate public or private bodies designated by Member States." ESD art. 3(4). The standards developed in each Member State must be recogized in all Member States. Id.

[101] Measures should be taken to ensure that: the data used to verify are the same as those displayed to the verifier; the E-signature is confirmed and that fact is indicated; the verifier can determine the contents of the data which is signed; there is a confirmation of the authenticity and validity of the certificate at the time the E-signature is verified; there is proper display of the verification and the subscriber's name (or pseudonym, if any); and any changes to the data are detectable. ESD Annex IV. Member States are charged to work with the EU Commission to develop and use secure signature-verification devices. ESD art. 3(6).

[102] ESD art. 4(1).

certificate is required to contain; assurance that the subscriber was in possession of the signature-creation data corresponding to the signature-verification data contained in the certificate, or identified in the certificate; and, when the CSP has generated both the signature-creation data and the signature-verification data, that those two sets of data have an interactive relationship.[103] CSP's are also obligated to maintain security of personal information received from the subscriber in the application for a certificate, and may not use the information for any other purpose without the subscriber's consent.[104] A qualified certificate issued by a CSP in a non-EU nation may be recognized within the EU if: the CSP is in compliance with the ESD's requirements and is accredited pursuant to a voluntary accreditation program established within a Member State; a CSP established within the EU has guaranteed the certificate; or this is provided by a bilateral or multilateral treaty.[105]

E-Signature Committee

An E-signature Committee ("Committee")[106] may be created to issue official standards for E-signature products.[107]

E-Government

Governments of the Member States should use E-signatures; if so, additional requirements may be imposed.[108] Specific governmental activities amenable to use of E-signatures include: purchasing, taxation, social security, health programs and the justice system.[109]

Implementation Matters

Each Member State must inform the Commission and other Member States information pertinent to: any voluntary accreditation program; name and address of the CSP regulator; name and address of the party responsible for preparation of standards for

[103] ESD art. 6(1). A CSP may also be liable for a relying third party's damages caused by the CSP's failure to give proper notice that a certificate has been revoked. ESD art. 6(2). However, a CSP may avoid liability if: he is able to prove he was not negligent; or the certificate's express limitations on purpose or value of the transaction have not been complied with. ESD art. 6(1), 6(3) and 6(4).
[104] ESD art. 8.
[105] ESD art. 7(1). In order to promote legal recognition of E-signatures generated outside the EU, the EU Commission will make proposals for implementation of standards and international agreements pertinent to certification services. ESD art. 7(2). If the EU Community encounters problems with market access in non-EU nations, the EU Commission may make proposals for negotiation of comparable rights for EU Member States in those nations. ESD art. 7(3).
[106] ESD art. 9. If a Member State has met these standards, it may presume it has complied with standards mentioned in ESD Annex II(f) and Annex III. ESD art. 3(5).
[107] ESD art. 10. E-signature products in compliance with the ESD's requirements must be allowed to circulate freely within the EU. ESD art. 4(2).
[108] ESD art. 3(7). Any additional requirements must be "objective, transparenent, proportionate and non-discriminatory," and must not be an impediment to "cross-border services for citizens." Id.
[109] ESD preamble 19.

signature-creation devices; and names and addresses of all accredited CSP's.[110] Each Member State was required to enact legislation necessary to accomplish the objectives of the ESD no later than 19 July 2001.[111] A review of the operation of the ESD was required to be completed by 19 July 2003; that review took into account technological and market developments, and harmonization of the ESD requirements in the Member States.[112]

The E-Commerce Directive

The European Union enacted the E-Commerce Directive (hereinafter "ECD") on 8 June 2000.[113] The ECD's purpose is to foster the free flow of E-commerce among the Member States.[114] Toward that end, the ECD contains: principles for Member States' E-commerce statutes; rules for certification service providers ("CSP"); rules for business communications and E-contracts; and provisions for liability of intermediaries, codes of conduct, dispute settlement resolution, litigation and Member State cooperation.[115] The ECD does not affect law pertinent to: public health; consumer rights; private international law and jurisdiction of courts; taxation; issues previously covered by Directives 95/46/EC and 97/66/EC; cartels; notaries public; representation of a client by an advocate, and defense of the client's rights in court; gambling activities; and measures taken "to promote cultural and linguistic diversity and to ensure the defence of pluralism."[116] The ECD refers to E-commerce as "information society services"[117] and refers to an E-commerce seller as a "service provider."[118] The ECD distinguishes a "recipient of the service"[119] and a "consumer."[120] Member States' laws pertinent to E-commerce or E-commerce service providers are referred to as "coordinated field."[121]

---

[110] ESD art. 11.
[111] ESD art. 13(1).
[112] ESD art. 12.
[113] European Union, DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 8 JUNE 2000 ON CERTAIN LEGAL ASPECTS OF INFORMATION SOCIETY SERVICES, IN PARTICULAR ELECTRONIC COMMERCE, IN THE INTERNAL MARKET ("ECD"); http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32000L0031&model=guichett.
[114] ECD art. 1(1).
[115] ECD art. 1(2).
[116] ECD preamble 11, 12, and 16; ECD art. 1(3)-(6).
[117] These are defined as "services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC." ECD art. 2(a).
[118] A service provider is defined as "any natural or legal person providing an information society service." ECD art. 2(b). However, the ECD distinguishes an ordinary service provider from an *established* service provider, defined as "a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period." The mere possession of the technical ability and technology necessary for provision of the service do not constitute establishment. ECD art. 2(c).
[119] This is defined as "any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible." ECD art. 2(d).
[120] This is defined as "any natural person who is acting for purposes which are outside his or her trade, business or profession." ECD art. 2(e).
[121] ECD art. 2(h). The coordinated field encompasses: service providers' qualification requirements which are a prerequisite to commencement of E-commerce activities; and rules regarding quality of service, E-

Member States' Supervision Requirements

Each Member State is responsible for ensuring that domestically-established service providers comply with the Member State's laws in the coordinated field.[122] A Member State may not use its laws in the coordinated field to restrict activities of service providers established in other Member States.[123] The two aforementioned sentences are inapplicable in some specified situations.[124] Each Member State must ensure that a service provider, before commencing its activities, has complied with all legal requirements.[125]

Service Providers' Requirements
Pertinent to General Information and Advertisement

Service providers are obliged to provide general information to customers and to the authorities; it must be easily and permanently accessible.[126] Service providers are obliged

---

contracts, advertising, and service providers' liability. ECD art. 2(h)(i). However, the coordinated field does not include: requirements concerning specific types of goods; delivery of goods; and rules concerning services provided non-electronically. ECD art. 2(h)(ii).

[122] ECD art. 3(1).

[123] ECD art. 3(2). However, a Member State does have the right to restrict activities of other Member States' service providers if this is necessary for: criminal law enforcement (especially laws pertinent to protection of minors, hate crimes, and protection of human dignity) maintenance of public health; national security and defense; and consumer protection (including investors). Before restriction is begun, the affected Member State must ask the other Member State (the one in which the service provider is established) to take action, and of its intention to restrict; if the other Member State refuses to take action, or takes inadequate action, the affected Member State may proceed with restriction, and the Commission must be informed. ECD art. 3(4). In an emergency, the affected Member State may restrict before giving notice to the other Member State and to the Commission, but they must be informed as soon as practicable of the action taken and the justification for it. ECD art. 3(5). Whereupon, the Commission will hold an inquiry as to the suitability of the affected Member State's action; if found to be "incompatible with Community law," the Commission will request the affected Member State from carrying out the restriction, or ending it expeditiously. ECD art. 3(6).

[124] ECD preamble 10 and art. 3(3). Those situations are: copyright; neighbouring rights; rights referred to in Directive 87/54/EEC and Directive 96/9/EC; industrial property rights; electronic money as referenced in art. 8(1) of Directive 2000/46/EC; article 44(2) of Directive 85/611/EEC; art. 30 and Title IV of Directive 92/49/EEC; Title IV of Directive 92/96/EEC; art. 7 and 8 of Directive 88/357/EEC; art. 4 of Directive 90/619/EEC; the freedom of contracting parties to choose the controlling law; contract rights pertinent to consumer contacts; the validity of contracts which create or transfer rights in real estate where those contracts must comply with the law of the Member State in which the real estate is located; and the issue of whether unsolicited E-mail advertising is permitted. ECD Annex.

[125] ECD art. 4(1). However, this is inapplicable to authorization rules which: are applied to all businesses (including those not engaged in E-commerce activities); or are applied pursuant to Directive 97/13/EC (relating to licenses of telecommunications services). ECD art. 4(2).

[126] ECD art. 5(1). The information is: name, address and contact information (including E-mail address) of service provider; name of trade register in which service provider is listed, and the trade register identification number (if applicable); the supervisory authority; professional license or designation, name of professional regulatory body, and reference to professional rules (if applicable); value-added-tax identification number (if applicable); and prices of services (and whether the price is inclusive of delivery expenses). ECD art. 5(1)-(2).

to provide additional information in electronic advertisements.[127] Member States may allow unsolicited E-mail advertisements, but special rules apply to them.[128] Professional service providers using E-mail communiques must abide by the rules of their profession pertinent to "independence, dignity and honour of the profession, professional secrecy and fairness toward clients and other members of the profession."[129]

E-Contracts

Member States must recognize the legal validity of E-contracts and must avoid creation of obstacles to their creation or utilization.[130] Member States must ensure that service providers provide clear and comprehensive information to the customer before the order is placed.[131] After the customer's order has been placed, the seller must promptly acknowledge the receipt of the order using electronic communications.[132]

Liability of Intermediaries

As a general rule, an intermediary (e.g., an internet service provider) is not liable for the content of the information if it is merely the information's: conduit;[133] cache;[134] or host.[135] Generally, an intermediary has no obligation to monitor the information.[136]

---

[127] ECD art. 6. The information is: designation that it is a commercial message; identification of the sender; identification of any discounts, premiums or gifts that are available (and clear explanation of how to qualify for them); and promotional competitions or games that are available (and the conditions for participation in them). Id.

[128] ECD art. 7. The advertisement: must be clearly identified as such; and must be capable of being opted-out of by the recipient (and the opt-out, if made, must be complied with by the service provider). Id.

[129] ECD preamble 32; ECD art. 8(1). Professional organizations are encouraged to adopt an EU code of conduct concerning the types of information allowed to be conveyed electronically. ECD art. 8(2). These codes of conduct will be taken into account by the Commission as they draft further rules pertinent to EU E-commerce. ECD art. 8(3). The ECD applies in addition to other EU Directives relating to professions. ECD art. 8(4).

[130] ECD preamble 34; ECD art. 9(1). However, a Member State may elect not to apply this provision to contracts concerning: creation or transfer of rights in real estate; a legal requirement for participation by the "courts, public authorities or professions exercising public authority;" granted suretyship, or "collateral securities furnished by persons acting for purposes outside their trade, business or profession;" or family law, or law of succession; ECD art. 9(2). If it elects not to apply the provision to one or more of those categories, it must so inform the Commission of the categories in question; furthermore, every five years the Member State must justify to the Commission why it is necessary to maintain those exceptions. ECD art. 9(3).

[131] ECD art. 10(1). The types of information to be provided are: how to consummate an E-contract; filing of the E-contact by the seller and its accessibility by the customer; how to correct input errors before the order is placed; the languages available; and any codes of conduct the seller has subscribed to (and how to get access to an electronic copy of them). ECD art. 10(1)-(2). These requirements are inapplicable to contracts consummated entirely by E-mail or by "equivalent individual communications." ECD art. 10(4). However, in all E-contracts, the seller must provide general contract terms and conditions to the buyer, and they must be capable of being stored and reproduced by him. ECD art. 10(3).

[132] ECD art. 11(1). A customer must be informed how to identify and correct input errors before the order is placed. ECD art. 11(2). The aforementioned requirements are inapplicable if the contract is consummated entirely by E-mail or by "equivalent individual communications." ECA art. 11(3). The order and acknowledgement of receipt are considered to have been received when they first become accessible. ECA art. 11(1).

[133] ECD art. 12.

Implementation

The Commission and the Member States should encourage the development of codes of conduct at the Community level and by trade, professional and consumer organizations; the purpose of such codes is to achieve more effective implementation of ECD art. 5-15.[137] Out-of-court settlement of E-commerce disputes is encouraged, and the ECD should not hamper Member States' informal dispute resolution procedures.[138] Statutes in the Member States governing civil court actions should enable an offended party to "terminate any alleged infringement and to prevent any further impairment of the interests involved."[139] Member States are mandated to cooperate with one another in the implementation of the ECD.[140] Member States were mandated to enact all laws and regulations necessary for implementation of the ECD by 17 January 2002.[141] Those laws and regulations were required to include a list of sanctions applicable to violators.[142] Those laws and regulations of the Member States may take into account the "linguistic diversity, national and regional specificities as well as their cultural heritage, and to ensure and maintain public access to the widest possible range of information society services."[143] Member States are required to take all measures necessary to enforce their laws and regulations.[144]

---

[134] ECD art. 13.
[135] ECD art. 14.
[136] ECD preamble 40-48; ECD art. 15. However, if the intermediary acquires knowledge that the information is illegal or offensive, there is an obligation to remove or disable access to the information. ECD art. 13(1)(e) and 14(1)(b).
[137] ECD preamble 49; ECD art. 16(1)(a) and 16(2).
[138] ECD preamble 51; ECD art. 17(1). Procedural safeguards for consumers should be established. ECD preamble 53; ECD art. 17(2). Bodies in the Member States responsible for out-of-court settlement of disputes should keep the Commission informed of significant decisions made, and should also inform the Commission of any "other information on the practices, usages or customs relating to electronic commerce." ECD art. 17(3).
[139] ECD art. 18(1).
[140] ECD art. 19(2). Member States should keep the Commission informed of any "significant or administrative judicial decisions" taken pertinent to implementation of the ECD, and the Commission should disseminate these to all Member States. ECD art. 19(5). Furthermore, Member States should cooperate with non-Member States in the development of compatible world E-commerce laws. (Yes! A "World Theory" is needed!) ECD preamble 61.
[141] ECD art. 22(1).
[142] ECD art. 20. The sanctions must be "effective, proportionate and dissuasive." Id.
[143] ECD preamble 63.
[144] ECD art. 20.

THE FORERUNNER OF GERMANY'S E-SIGNATURE ACT: THE DIGITAL SIGNATURE ACT

Germany was the first member of the European Union to enact a digital signature law.[145] The Digital Signature Act (hereinafter "DSA") was effective from 1997 until 2001[146] and was enforced by the Minister of Telecommunications ("Minister"),[147] who was empowered to issue regulations for its implementation.[148] The purposes of the DSA were to establish standards for security of digital signatures and to facilitate the detection of forged digital signatures.[149] A digital signature was defined as "a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided by a signature key certificate of a certification authority. . ."[150]

Certification Authorities

A certification authority ("CA") was defined as a "natural or legal person who certifies the assignment of public signature keys to natural persons and to this end holds a license."[151] CA's issued certificates[152] and provided time-stamping[153] services. All CA's were mandated to be licensed; a license was not issued by the Minister unless the applicant demonstrated sufficient knowledge of computer security and submitted a copy of the standard operating procedures to be employed in its business.[154] The Minister issued a certificate to each CA to support its private key, which in turn was used by the

---

[145] Andrew B. Berman, Note, "International Divergence: The 'Keys' to Signing on the Digital Line—The Cross-Border Recognition of Electronic Contracts and Digital Signatures," 28 SYRACUSE J. INT'L L. & COM. 125, 149 (2001).

[146] Federal Republic of Germany, ACT ON DIGITAL SIGNATURE ("DSA"), 1997; http://www.iuscomp.org/gla/statutes/SiG.htm .

[147] DSA s 3.

[148] DSA s 16.

[149] DSA s 1(1). Since digital signatures are not required to be used, the use of other security procedures not mentioned in the DSA is not mandatory. DSA s 1(2).

[150] DSA s 2(1).

[151] DSA s 2(2). Under the DSA, all CA's were required to be licensed. DSA s 4(1). Hence, Germany was a compulsory jurisdiction. This was changed by the ESA, enacted in 2001.

[152] A certificate was defined as "a digital certificate bearing a digital signature and pertaining to the assignment of a public signature key to a natural person (signature key certificate) or a separate digital certificate containing further information and clearly referring to a specific signature key certificate (attribute certificate)." DSA s 2(3).

[153] A time stamp was defined as "a digital declaration bearing a digital signature and issued by a certification authority confirming that the specific digital data were presented to it at a particular point in time." DSA s 2(4). Upon request, a CA attached a time stamp to an E-document. DSA s 9.

[154] DSA s 4(2)-(3). A CA was required to maintain documentation of its mandated security procedures. DSA s 10. A CA had to abide by the requirements established by the DSA and related regulations. The Minister had the right to enter the CA's worksite for purpose of inspection of its equipment, documentation and books. If a CA failed an inspection, a CA's license could be revoked; whereupon, the CA's duties would be transferred to another CA. The revocation of a CA's license would not affect the validity of certificates issued before the revocation became effective. DSA 13. During the inspection, the Minister would also check to see if the CA's computer information system was in compliance with mandated technical standards. DSA s 14.

CA to affix its digital signature to each certificate issued to its subscribers; the Minister also maintained a register of licensed CA's, their contact information, and certificates they issued.[155] A CA confirmed the identity of every subscriber who applied for a certificate,[156] and made the certificate (and the public key contained therein) available for inspection by relying third parties at the CA's website.[157] At an applicant's request, the certificate could state that the applicant is an agent of a third party and contain proof that the third party had consented to the agency relationship.[158] The subscriber was allowed to use a fictitious name instead of his real name.[159] A CA was required to inform each subscriber: the technical security requirements; how to use the private key; and that "data bearing a digital signature may need to be signed again before the security of the existing signature decreases with time."[160] A certificate previously issued could be revoked by a CA if good cause existed.[161] A CA was required to inform the Minister if it planned to go out of business, and had to locate another CA to assume its duties; whereupon, its certificates would be given to the other CA, or to the Minister.[162] Certificates issued by foreign CA's were legally recognized in Germany, provided: the CA was in one of the member states of the European Union; the CA was in a nation which is a party to the Agreement on the European Economic Area; or the CA was in a nation which had entered into a treaty with Germany concerning reciprocal recognition of certificates.[163]

GERMANY'S ELECTRONIC SIGNATURE ACT

The Electronic Signature Act (hereinafter "ESA") was enacted in 2001 to replace the DSA and to comply with all of the requirements of the European Union's E-Signatures

---

[155] DSA s 4(5).

[156] In confirming the applicant's identity, the CA was only allowed to collect information directly from the applicant; information was not allowed to be collected from third parties without the consent of the applicant. Furthermore, the collected information could only be used to confirm the applicant's identity, and could not be used for any other purpose. DSA s 12(1).

[157] DSA s 5(1). Each certificate was required to contain the following: name (or pseudonym) of subscriber; name of issuing CA; public key; names of the algorithms with which the public keys of the subscriber and the CA could be used; certificate number of certificate; period of validity; and any limitations on purpose of use or value of transaction. DSA s 7(1). Information concerning an agency relationship or admission to professional practice could be included in a "signature key" certificate, an "attribute" certificate, or both. DSA s 7(2). No additional information could be listed in a "signature key" certificate unless all parties were in agreement. DSA s 7(3).

[158] DSA s 5(2).

[159] DSA s 5(3). If requested by law enforcement or intelligence services, the real name of the subscriber had to be divulged by the CA, and this action was required to be documented; if that happened, the subscriber had to be informed immediately. DSA s 12(2).

[160] DSA s 6.

[161] DSA s 8. Grounds for revocation include: request of subscriber, or a third party whose information is contained in the certificate; applicant giving inaccurate information to CA; CA goes out of business without finding another CA to assume its operations; revocation of license of CA; and order of Minister. DSA s 8.

[162] DSA s 11(1)-(2). A CA is required to go out of business if it becomes the subject of a bankruptcy or dissolution proceeding. DSA s 11(3).

[163] DSA s 15.

Directive.[164] Like the DSA before it, the ESA is also enforced by the Minister of Telecommunications ("Minister").[165] The federal government is empowered to enact additional regulations necessary for implementation of the ESA[166]. An E-signature is defined as "data in electronic form that are attached to other electronic data or logically linked to them and used for authentication."[167]

Certification Service Providers

Unlike the CA's under the DSA, a certification service provider ("CSP") is not required to be accredited.[168] Although accreditation is not required, a CSP may voluntarily seek accreditation of its operations from the Minister.[169] For a CSP to issue a qualified certificate[170] in support of a qualified E-signature, stringent security[171] requirements must be met such that any subsequent alteration of the attached data is detectable.[172] A CSP is mandated to have a publicly-accessible register allowing ascertainment of the status of certificates.[173] A CSP is obligated to cancel a qualified certificate if: the subscriber so requests; it was issued under false pretenses; the CSP goes out of business and its operations are not taken over by another CSP; if the Minister so orders;[174]or, if the

---

[164] Federal Republic of Germany, LAW GOVERNING FRAMEWORK CONDITIONS FOR ELECTRONIC SIGNATURES AND AMENDING OTHER REGULATIONS ("ESA"), 21 May 2001; http://www.signaturbuendnis.de/englisch/legalrequirements/ElectronicSignatureAct.pdf. The ESA went into effect on 1 January 2002. ESA art. 5.

[165] ESA ss 3 and 21.

[166] ESA s 24.

[167] ESA s 2(1). The ESA distinguishes an advanced E-signature from a qualified E-signature. An advanced E-signature is one that is: assigned only to one subscriber; capable of being identified as the subscriber; generated using a method under the sole control of the subscriber; and liked to the attached data so that any alteration of the data is detectable. ESA s 2(2). A qualifed E-signature is an advanced E-signature that is: supported with a qualified certificate; and generated with a secure signature creation device. ESA s 2(3).

[168] ESA s 4(1). Nevertheless, the CSP must be able to demonstrate to the Minister that it possesses sufficient reliability, knowledge of security methods, and insurance coverage. ESA s 4(2). If a CSP ceases to have these attributes, the Minister may temporarily order it to close operations until its deficiencies are rectified. ESA s 19(3).

[169] ESA s 15. If accreditation is granted, the Minister will issue a qualified certificate to be used by the accredited CSP in its operations. ESA s 16(1). The Minister will maintain an online registry of accredited CSP's which may be accessible by the general public. ESA s 16(2).

[170] A qualified certificate must contain: the certificate number; the period of validity; the name of the CSP and its nation or state of domicile; the name of the subscriber (and pseudonym and other attributes, if applicable); the public key, designated by the ESA as the "signature test code;" the algorithms which correspond to the public key of the subscriber and of the CSP; any limitations on purpose or value of transactions; and a statement that it is a qualified certificate. ESA s 7(1).

[171] Secure signature creation devices and secure signature-application components must be used. ESA s 17. To ensure this occurs, the devices used must be approved by a recognized testing and confirmation office. ESA ss 17(4) and 18.

[172] ESA s 5(4). The applicant who has applied for issuance of a qualified certificate must present positive confirmation of his identity to the CSP. ESA s 5(1). The CSP must maintain confidentiality of all information pertinent to the subscriber. ESA s 14. Before issuance of the qualified certificate, the CSP must inform the applicant; how to generate the E-signature; the legal ramifications of using an E-signature; and the subscriber's duty to maintain security over the private key. ESA s 6.

[173] ESA s 10.

[174] ESA s 8(1)

subscriber is an agent of a principal, and the principal so requests.[175] If a relying third party suffers damages due to a CSP's failure to abide by the ESA, then the CSP is liable to that third party, unless: the third party knew some of the information in the certificate was inaccurate; any limitations expressed in the certificate were violated; or the CSP was not culpable.[176] A CSP going out of business must give notice to the Minister and look for another CSP to assume its responsibilities.[177] All CSP's are required to cooperate with the Minister during inspections of the worksite.[178] A fine may be assessed against a CSP for failure to abide by its obligations under the ESA.[179] A qualified certificate issued by a foreign CSP may be recognized under certain conditions[180] if the E-signature products are in compliance with requirements of the ESA.[181]

MULTIMEDIA LAW

The Multimedia Law (hereinafter "MML") was enacted in 1997.[182] The statute's purpose is "to create uniform economic conditions for the various uses of electronic information and communications services."[183] *Inter alia*, the MML covers the rights and responsibilities of internet service providers,[184] informational rights of cusomers of internet service providers,[185] and enforcement of confidentiality obligations of internet service providers.[186]

RECOMMENDATIONS FOR IMPROVEMENT OF GERMAN E-COMMERCE LAW

Germany has made a satisfactory beginning in its E-commerce law. However, it has not gone far enough; the following changes should be considered.

---

[175] ESA s 8(2).
[176] ESA s 11.
[177] ESA s 13.
[178] ESA s 20.
[179] ESA s 21.
[180] ESA s 23(1). An E-signature supported with a qualified certificate issued by a CSP domiciled in another member state of the E.U. is recognized in Germany. Furthermore, an E-signature supported with a qualified certificate issued by a CSP not domiciled in the E.U. is recognized in Germany if the CSP meets the requirements of the E-Signature Directive and: it has accredited status in an E.U. nation; or another CSP domiciled in the E.U. guarantees the certificate; or recognition is provided under an international treaty. Id. In all of the aforementioned cases, the degree of security must be equivalent to that of domestic CSP's. ESA s 23(2).
[181] ESA s 23(3).
[182] Federal Republic of Germany, FEDERAL LAW TO REGULATE THE CONDITIONS FOR INFORMATION AND COMMUNICATIONS SERVICES ("MML"), 29 June 1997; http://www.kuner.com/data/reg/multimd3.htm.
[183] MML s 1.
[184] MML ss 4-6.
[185] MML s 7.
[186] MML s 8.

Enact a Comprehensive Electronic Transactions Law

All of the laws pertinent to electronic transactions should be included under the umbrella of the new Electronic Transactions Law ("ETL"). A comprehensive statute is easier for all affected parties to research and to comprehend; accordingly, other existing laws pertinent to electronic transactions should be consolidated in the ETL.

The ETL should include the following sections: Introduction; Legal Recognition of Electronic Form and Secure Electronic Documents and Signatures; Legal Presumptions, Admissibility and Evidential Weight of Electronic Evidence in a Court of Law or Administrative Proceeding; Use of Electronic Form to Comply With Requirements of Other Statutes; Regulation of Certification Service Providers; Duties and Liabilities of Certification Service Providers; Duties of Subscribers and Relying Third Parties; Electronic Contracts; Consumer Protections in E-Commerce Transactions; Computer Crimes; Computer Criminal and Civil Justice; E-Government; Domain Name Registration; Network Intermediaries; Privacy of Information; and Other Issues.

Make the ETL Supreme In All Things Electronic

If the ETL is in conflict with another law or statute, the ETL should prevail.

Add: A List of Other Laws Affected by the ETL

There should be a list of other statutes and regulations that are modified or affected by the ETL. Additionally, there should be a list of the names of all other statutes currently in force (and the applicable provisions in each) which can be complied with using the electronic form instead of the paper form.

Delete: All Exclusions

The Electronic Signature Law should explicitly eliminate any expressed or implied exclusions from coverage. This would recognize the legal validity of electronic documents in all situations, except when the parties have made a contrary agreement. This would firmly tell the world that Germany sees virtually no limits to the utilization of the electronic form and would hasten the adoption of the electronic form by its citizens and residents. Only a few nations have completely eliminated exclusions in their E-commerce statutes,[187] and none of them are in Europe.

---

[187] For example, Azerbaijan's statute contains no exclusions from coverage; it states that electronic documents "can be used (applied) in *all activity spheres* where software and technical equipment could be applied to create, use, store, transmit and receive information." Republic of Azerbaijan, ELECTRONIC DOCUMENT LAW, 2003, art. 1(1) (emphasis added), note 67 supra. Iran, Montenegro, New Zealand and Tunisia also have no exclusions from coverage. *See* Islamic Republic of Iran, ELECTRONIC COMMERCE LAW OF THE ISLAMIC REPUBLIC OF IRAN, 2003 <http://irtp.com/laws/ec/IR%20Iran%20E-Commerce%20Law.pdf>; Republic of Montenegro, ELECTRONIC SIGNATURE LAW, 2003 <www.mipa.cg.yu>; Commonwealth of New Zealand, ELECTRONIC TRANSACTIONS ACT 2000

Add: Legal Validity of Electronic Form To Comply
With Several Additional Requirements of Other Statutes

The ETL should state a general presumption that the electronic form may be used to satisfy requirements contained in other statutes which are prerequisite to incurrence of a legal right. Those requirements include, but are not limited to, the following: the witnessing of a handwritten signature or seal; a paper document's notarization, certification, acknowledgement, verification, attestation, or being made under oath; production of multiple copies of a paper document (where production of one electronic copy is sufficient); communication by registered or certified mail (provided that the electronic message is transmitted thorough the sender's Certification Authority and confirmed by him); and seller's provision of a notice to a consumer in writing. For a comprehensive list of such electronic compliance allowances, refer to the New Zealand statute.[188]

Add: E-Contract Rules

As mentioned, Germany should include comprehensive E-contract rules in its new Electronic Transactions Law. These rules should include carriage contracts and automated contracts, and others. For carriage contracts, Colombia's Electronic Trade Law has a commendable paradigm.[189] For automated contracts, the U.S. Uniform Electronic Transactions Act contains a good model.[190]

Add: Consumer Protections for E-Buyers

Germany needs to enact a general consumer protection statute applicable to all internet consumers. The Republic of Tunisia can be used as a model for good consumer protections. The Tunisian E-commerce statute gives consumers: (1) a "last chance" to review an order before it is entered into; (2) a 10-day window of opportunity to withdraw from an agreement after it has been made; (3) a right to a refund if the goods are late or if they do not conform to specifications; and (4) no risk during the 10-day trial period after goods have been received. Tunisian E-consumers enjoy some of the best protections in the world.[191]

<http://www.med.govt.nz/templates/MultipageDocumentPage____9779.aspx>; and Republic of Tunisia, ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE LAW, 9 August 2000 <http://www.bakernet.com.org>.

[188] Id. at fourth citation.

[189] Note 71 supra.

[190] Note 59 supra. *See* Stephen E. Blythe, Note 58 supra (both citations).

[191] Note 86 supra. One of the few nations that may offer better consumer protections is Korea. That country has enacted a separate statute specifically for E-commerce consumer protections—the E-Commerce Transactions Consumer Protection Act. *See* Korean Legislation Research Institute, Act on the Consumer Protection in the Electronic Commerce Transactions ("CPA"), STATUTES OF THE REPUBLIC OF KOREA, Vol. 13, pp. 481 to 485-30. Originally enacted by Law No. 6687 (30 March 2002), and amended by Act Nos. 7315 and 7344 of 31 December 2004 and 27 January 2005, respectively. The CPA recently underwent a major overhaul with substantial amendments in Act No. 7487 of 31 March 2005; those amendments became effective on 1 April 2006. For an analysis of the CPA, *see* Stephen E. Blythe, Note 84 supra. Iran also provides good consumer protections, including a window of opportunity to withdraw from

Add: I.T. Courts for E-Commerce Disputes

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 them. 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 Nepal can be used as a model.[192]

Add: Long-Arm Jurisdiction Against Foreign E-Commerce Parties

Because so many of the E-commerce transactions incurred by the residents of Germany will be with parties outside the borders of Germany, it would be prudent for the new ETL to explicitly state its claim of "long arm" jurisdiction against any E-commerce party who is a resident or citizen of a foreign jurisdiction, so long as that party has established "minimum contacts" with Germany. The Kingdom of Tonga's statute can be used as a model.[193]

Minimum contacts will exist if a cyber-seller outside of the country makes a sale to a person in Germany. In that situation, German laws should be applicable to the foreign party because that party has had an effect upon the country through the transmission of an electronic message that was received in Germany. The foreign party should not be allowed to evade the jurisdiction of the German courts merely because he is not physically present in the country. After all, E-commerce is an inherently international and multi-jurisdictional phenomenon.

Add: National ID Card With Digital Signature

Germany should adopt a National ID Card. It would contain several types of personal information, including voter registration.[194] Application and other information pertinent to the National ID Card should be made available at the Government Portal. Only a handful of other jurisdictions have adopted an ID card; they include Belgium[195] and Hong

---

an E-commerce transaction previously entered into; however, the window in Iran is only seven days, as opposed to Tunisia's ten days. *See* Stephen E. Blythe, Note 77 supra.

[192] Note 53 supra.

[193] The Republic of Tonga explicitly states its claim of long-arm jurisdiction over foreign E-commerce parties. *See* Stephen E. Blythe, Note 88 supra.

[194] Privacy International, PHR2006: THE HASHEMITE KINGDOM OF JORDAN, 18 December 2007, p.2; http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559523 .

[195] By 2010, Belgium will have issued an electronic ID card to each of its 9 million inhabitants, becoming the first European nation to carry out this achievement. Each resident will pay approximately EU 10 for his card. These cards contain two E-signatures; one will be used for identification of the holder, and the other will be used to sign E-documents. Already, the electronic ID card is being used for: access to the Belgian

Kong.[196] In those jurisdictions, the ID Card's computer chip can serve as the E-signature of the cardholder.[197] This idea is recommended for adoption in Germany.

Add: Germany's Post Office To Become an Accredited Certification Service Provider

In order to promote the utilization of E-signatures among the general public and to make them cheaper and more accessible, the German Post Office should be designated as a licensed CSP. For a model, look to the Belgian Post Office, which has implemented a promotional campaign to educate the general public about E-signatures and their availability through its Post Office.[198]

Add: Several New Computer Crimes

The list of computer crimes needs to be expanded. The following computer crimes, with appropriate penalties, should be recognized: (a) Unauthorized Tampering with Computer Information; (b) Unauthorized Use of a Computer Service; (c) Unauthorized Interference in the Operation of a Computer; (d) Unauthorized Dissemination of Computer Access Codes or Passwords; and (e) Injection of a Virus into a Computer. The Singapore Computer Misuse Act can be used as a model.[199]

SUMMARY AND CONCLUSIONS

The Internet and E-Commerce in Germany

During the past decade, Germany experienced rapid growth in internet broadband accessibility and E-commerce. Although that growth rate has recently begun to taper off,

---

government website and its E-government services; signing of legal documents in digital form (e.g., tax declaration, VAT declaration, and social security affirmations); access to community container parks; parking tickets; signing of registered mail; signing of Flemish Parliament Decrees; requests for official documents and access to National Register records; and access to the E-library service. Additionally, Dell, HP and Siemens computers are now able to read the Belgian ID card and to process its E-signature data. Interdisciplinary Centre for Law & Information Technology, THE LEGAL AND MARKET ASPECTS OF ELECTRONIC SIGNATURES, 2003, pp. 177-178; http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf.

[196] Rina C.Y. Chung, Note 20 supra. For information pertinent to the Hong Kong I.D. card, refer to the Hong Kong Government Portal; http://www.smartid.gov.hk/. The list of other nations which have adopted national ID cards includes: Austria, Bahrain, Belgium, Hong Kong, Israel, Italy, Jordan, Spain and the United Arab Emirates.

[197] Rina C.Y. Chung, Note 20 supra.

[198] Kingdom of Belgium, LEGAL FRAMEWORK FOR ELECTRONIC SIGNATURES AND CERTIFICATION SERVICES ("ESA"), 9 July 2001. This statute was supplemented by the ROYAL DECREE ORGANIZING THE SUPERVISION AND ACCREDITATION OF CERTIFICATION SERVICE PROVIDERS ISSUING QUALIFIED CERTIFICATES, 6 December 2002.

[199] Republic of Singapore, COMPUTER MISUSE ACT (Cap. 50A), 30 August 1993; http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_gettopo.pl?actno=1998-REVED-50A. *See* Stephen E. Blythe, Note 62 supra, second citation.

it is expected to remain relatively high during this decade. However, in order for German E-commerce to maximize its potential, its E-commerce laws need to be updated.

Electronic Signatures

An E-signature is used to sign an electronic document. There are several types of E-signatures: 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. The most secure of these is the digital signature because it will freeze the contents of the message to which it is attached and will indicate if the message has been altered since its creation. Because of the high degree of security it offers and its assurance that an attached document has not been altered, the digital signature is the most preferred and is given the highest degree of legal status. However, biometric E-signatures (e.g., a retinal scan) are also very useful and are often employed in conjunction with the digital signature.

Three Generations of E-Signature Law

There have been three generations of E-signature law since the world's first E-signature statute was enacted in 1995. These three successive generations emphasized, respectively: exclusive recognition of public key infrastructure ("PKI") technology and the digital signature; technological neutrality, with all types of E-signatures and technologies recognized; and a hybrid perspective which recognized all types of E-signatures, with a preference shown for PKI in admission of E-signatures and electronic documents ("E-documents") into evidence.

The Foundation of German E-Commerce Law: the European Union Directives

The E-Signature Directive established a common framework for the development of E-signature law in the EU, and thereby promotes the legal recognition of E-signatures and their greater use. Only an advanced E-signature (supported with a qualified certificate and created by a secure private key) is considered to be fully legally equivalent to a handwritten signature, but all E-signatures are potentially admissible into evidence in court. CSP's are not mandated to be licensed or to be accredited, but all CSP's who issue qualified certificates must be regulated and must meet more stringent qualifications than CSP's who do not issue qualified certificates. CSP's bear potential legal liability for: the information contained in a qualified certificate; ensuring that the subscriber is in possession of the private key; ensuring that the private key and the public key have an interactive relationship; and maintaining the confidentiality of the subscriber's private information. Three grounds are provided for the recognition of a qualified certificate issued by a CSP in a non-EU nation. E-government is encouraged and a committee was established to promulgate standards for E-signature products.

The goal of the E-Commerce Directive ("ECD") is to promote the development of E-commerce in the EU. The ECD contains a framework for the Member States' E-commerce statutes. Accordingly, rules are proposed pertinent to: CSP's; E-contracts; intermediaries' liability and codes of conduct; dispute settlement; and litigation. A number of areas are excluded from coverage of the ECD, e.g., public health, taxation, notaries public, and gambling. Each Member State is responsible for regulation of its E-sellers and may not restrict the activities of E-sellers established in other Member States. E-sellers are mandated to: provide full information in advertisements (professionals must abide by their professional advertising standards); and promptly acknowledge receipt of an order. An internet service provider is not legally liable for content of information if it is a mere conduit, cache or host.

Germany's Digital Signature Act: The Forerunner of the German E-Signature Act

The Digital Signature Act ("DSA") was a first-generation E-signature law; the only type of E-signature with legal recognition was the digital signature. Noteworthy aspects included the provisions related to: technical standards of the CA's computer information system; statement of an agent's name on a certificate; a need to periodically re-sign an E-document in order to maintain a high degree of security; and a CA's duty to disclose the real name of a subscriber that is using a pseudonym if requested to do so by law enforcement or intelligence authorities.

Germany's Electronic Signature Act

The Electronic Signature Act replaced the DSA in 2001 in order to meet the requirements of the European Union's E-Signatures Directive and has the following notable attributes: requirements for voluntary accreditation of a CSP; requirements to use secure signature creation devices and secure signature-application components, with provision that only a recognized testing and confirmation office can be used to attest to that fact; and the requirements pertinent to recognition of foreign CSP's and the products used by them.

Germany's Multimedia Law

The Multimedia Law regulates internet service providers and provides for enforcement of their obligation to maintain confidentiality over information pertinent to their customers.

Recommendations for Improvement of the German E-Commerce Statutes

The German E-commerce statutes should be refined and supplemented as follows: (1) enact a comprehensive Electronic Transactions Act ("ETA"); (2) make the ETA supreme in all things electronic; (3) add a list of other German laws affected by the ETA, which would be invaluable to anyone researching German E-commerce law; (4) delete all exclusions from coverage, which would open the door for the electronic form to be used in virtually all situations; (5) recognize the legal validity of the electronic form in order to comply with several additional requirements of other statutes; (6) add E-contract rules

relating to automated contracts and electronic carriage contracts; (7) add additional consumer protections for E-buyers; (8) add I.T. Courts for resolution of E-commerce disputes; (9) add explicit long-arm jurisdiction over foreign E-commerce parties; (10) add Germany's Post Office as an accredited CSP; (11) add Registration Agents to assist CSPs; (12) require a National ID Card, which would contain a computer chip with a digital signature that could be activated by a CSP; and (13) enact several new computer crimes, including Intentional Injection of a Virus Into a Computer System.