Eur J Law Econ (2008) 26:75–103
DOI 10.1007/s10657-008-9053-y

Croatia's computer laws: promotion of growth in E-commerce via greater cyber-security

Stephen E. Blythe

Published online: 12 June 2008

Abstract Croatia's *Electronic Signature Act ("ESA")* was enacted in 2002. The ESA is third-generation and provides for legal recognition of all types of E-signatures, but gives preferred status to the digital signature. The ESA provides for regulation of Certification Authorities ("CA"), who may voluntarily elect to become accredited if they are able to comply with stringent financial and technical requirements. The principal duties of CA's are to: issue certificates to successful applicants; confirm the authenticity and integrity of E-signatures to relying third parties; maintain a repository of certificates which may be accessed by the public; and cancel a certificate if any information contained therein is discovered to be inaccurate. The ESA covers legal liability of CA's and punitive measures which may be taken against them if they violate the ESA. The *Electronic Document Act ("EDA")* was enacted in 2005. The EDA specifies how an E-document can be used to comply with a statutory requirement for production of a paper document or an original document. The EDA also creates a legal presumption of admissibility of evidence in electronic form, and contains rules pertinent to assumed time/place of transmission/receipt of an E-message. The EDA covers liability of Internet service providers and specifies several computer crimes.

Stephen E. Blythe is a Professor of Law and Accounting, New York Institute of Technology, CERT Technology Park, Abu Dhabi, United Arab Emirates. Ph.D. Candidate (Int'l E-Commerce Law), The University of Hong Kong (China); Ph.D. (Business Administration), University of Arkansas, 1979; J.D. *cum laude*, Texas Southern University, 1986; LL.M. (Int'l Bus. Law) University of Houston, 1992; LL.M. (Info. Tech. Law) *with distinction*, University of Strathclyde (Scotland), 2005. Attorney at Law, Texas and Oklahoma; C.P.A., Texas. He practiced solo (employment-discrimination litigation) in Houston, Texas, was affiliated with the Cheek Law Firm (insurance-defense litigation) in Oklahoma City, and was a management consultant for the city of Haikou, China. Additionally, he has taught law, accounting, management, economics and international business at 15 universities located in the United States, Africa and the Middle East.

S. E. Blythe (✉)
School of Management, New York Institute of Technology, CERT Technology Park, Al Muroor Road, P. O. Box 5464, Abu Dhabi, UAE
e-mail: itlawforever@netscape.net

The *Electronic Commerce Act ("ECA")* was enacted in 2003. The ECA provides for basic E-contract rules, basic regulation of E-commerce sellers, and basic consumer protections of E-commerce buyers. Although it was a satisfactory first-step, the ECA needs to be fine-tuned with the following modifications: (1) add E-contract attribution rules; (2) improve the E-contract acknowledgement-of-receipt rules; (3) add E-contract rules for carriage contracts; (4) strengthen the consumer protections of E-commerce buyers; (5) establish information technology courts for resolution of E-commerce disputes; (6) add cybersuite provisions; and (7) add explicit long-arm jurisdiction over foreign E-commerce sellers.

Keywords EU · Directives · Croatia · E-signature · E-commerce · E-document

JEL Classification K29

1 Objectives of the article

The objectives of this article are to: (1) introduce the reader to Croatia's economy and Internet usage; (2) explain the role of electronic signatures, cryptology, public key infrastructure, and certification authorities; (3) cover the three generations of electronic signature law; (4) describe the European Union's E-Signatures Directive and E-Commerce Directive; (5) analyze Croatia's E-Signature Act, E-Commerce Act and E-Document Act; and (6) make recommendations for improvement of Croatian computer laws.

2 Croatia's economy and the Internet

Croatia was part of the old Austro-Hungarian Empire until the end of World War I. In 1918, the Croats, Serbs and Slovenes united to form a kingdom which assumed the name of Yugoslavia in 1929. Yugoslavia fell under the control of the Soviet Union after World War II with strongman Marshal Tito as its leader. Following the collapse of the Soviet Union, Croatia declared independence in 1991 but had to endure four years of armed conflict before it drove out Serbian military forces.[1] During those 4 years, Croatia's once-thriving economy collapsed and the instability of the country caused it to miss an opportunity to get an early influx of external investment capital.[2]

After 2000, Croatia's economy began a slow recovery. During this decade, Croatia has had a moderate annual rate of economic growth—between 4 and 6%. The nation's gross domestic product ("GDP") was estimated to be US $70 billion in 2007. This growth has been largely due to an increase in tourism and a rise in consumer spending on credit.[3] Croatia's primary exports are transportation

[1] U.S. Central Intelligence Agency ("CIA"), THE WORLD FACTBOOK, "Croatia," 20 March 2008, p. 1; http://www.cia.gov/library/publications/the-world-factbook/print/hr.html.

[2] Id. at 5–6.

[3] Id. at 6.

equipment, textiles, chemicals, foodstuffs and fuels, and their annual value was recently estimated to be US $12 billion.[4]

In spite of the modest recovery of the economy, the rate of unemployment has remained high, estimated at 11.8%.[5] Additionally, 11% of Croatians are impoverished.[6] The trade deficit is growing and the nation has pockets of uneven economic growth. To combat its unemployment, poverty and trade deficit problems, Croatia needs to pursue structural economic reforms in order to become more competitive in the global economy. Unfortunately, needed reforms such as privatization have often been opposed by the general public and have had little support from Croatian politicians. However, it is expected that these economic reforms will be achieved within the next few years because Croatia has recently been designated an "official candidate country" for membership in the European Union ("EU"), and these reforms will be necessary in order to qualify for admission to the EU.[7]

Croatia has more than 260,000 Internet hosts and 9 Internet service providers.[8] Thirty-five percent of Croatians—1.6 million out of a population of 4.5 million—use the Internet.[9] Since the number of Internet users continues to increase, the number of E-commerce transactions is also expected to rise. Additionally, Croatia's new computer laws—the focal points of this article—have created a sound legal infrastructure and heightened security requirements for electronic transactions, further bolstering the growth of E-commerce in Croatia.

3 Electronic signatures

Contract law worldwide has traditionally required the parties to affix their signatures to a document.[10] With the onset of the electronic age, the electronic signature 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,"[11] 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."[12] An electronic signature may

[4] Id. at 7.

[5] Id. at 6.

[6] Id. at 10.

[7] Id. at 6, and note 79 infra.

[8] Id. at 8.

[9] Id. at 2 and 8.

[10] See United States of America (1998).

[11] Smedinghoff (1999).

[12] European Union, E-SIGNATURES DIRECTIVE, note 80 infra, art. 2(1). Under Croatian law, an electronic signature is defined as "a set of data in electronic form which are associated or logically connected with other data in electronic form and which serve to identify the signatory and the authenticity of the signed electronic document." ESA, note 140 infra, art. 2(1). An electronic document is defined in Croatia as "a complete set of data which is electronically generated, sent, received or stored on electronic, magnetic, optical or other media". The content of an electronic document shall encompass all forms of written or other text, data, images and drawings, maps, sound, music, speech and computer databases. ESA, note 140 infra, art. 2(4).

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.[13]

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."[14] 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.

3.1 Online contracts: four levels of security

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

a. The first level would exist if a party accepted an offer by merely clicking an "I Agree" button on a computer screen.[15]
b. 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.[16]
c. 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 voice pattern, face recognition, a scan of the retina or the iris within one's eyeball, a digital reproduction of a fingerprint,[17] 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.[18] For example, if a person's handwriting was being used as the biometric identifier, 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.[19]

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

[13] Tang (1999).

[14] Dessent (2002).

[15] Stern (2001).

[16] Id.

[17] In the highly successful Hong Kong Identity Card, the two thumb prints are used as a biometric identifier. See Rina (2003).

[18] Note 15 supra at 395–96; and CYBER-SIGN.

[19] Id.

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;"[20] 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.[21] The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers.[22] Many also recommend the use of both methods; this was the course taken by the Hong Kong government in designing its identity card.[23]

d. 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.[24] It is "the sequence of bits that is created by running an electronic message through a one-way hash function and then encrypting the resulting message digest with the sender's private key."[25] 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.[26]

3.2 Digital signature technology: public key infrastructure

The technology used with digital signatures is known as public key infrastructure, or "PKI."[27] PKI consists of four steps:

[20] Pun et al. (2002).

[21] Id. at 257.

[22] 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 (covered infra) 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 Wright (2001).

[23] Note 17 supra.

[24] 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 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 (2000).

[25] Note 11 supra at 146.

[26] Poggi (2000).

[27] Fischer (2001).

a. The first step in utilizing this technology is to create a public–private key pair; the private key[28] will be kept in confidence by the sender,[29] but the public key[30] will be available online.[31]
b. 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. Asymmetric encryption provides one of the highest—if not *the* highest—degrees of security in electronic transactions. The encrypted hash function is the "digital signature" for the document.[32]
c. The third step is to attach the digital signature to the message and to send both to the recipient.
d. 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.[33] If they match, the recipient knows the message has not been altered.[34]

3.3 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."[35] Although a handwritten signature is only

[28] Under Croatian law, the private key is considered to be part of the "electronic signature development data," which is defined as "the unique data, such as the codes or the private encryption key which the signatory uses to generate the electronic signature." ESA, Note 140 infra, art. 2(5).

[29] American Bar Association (2001). Under Croatian law, the sender is the person signing the electronic document; that person is labeled a "signatory." A signatory is defined as "a person who possesses the means to generate the electronic signature and to sign therewith, and who acts either on his or her own behalf or on behalf of the natural or legal person that he or she represents." ESA, Note 140 infra, art. 2(3).

[30] Under Croatian law, the public key is considered to be one of the "signature verification data," defined as "data such as codes or public encryption keys which are used for the purpose of verifying electronic signatures." ESA, Note 140 infra, art. 2(8).

[31] Note 13 supra at 305.

[32] Note 26 supra at 249.

[33] American Bar Association, Section of Science & Technology, Information Security Committee (1995, 1996).

[34] Zaremba (2003).

[35] Note 26 supra at 250.

"signatory-specific," the digital signature is both "signatory-specific" and "document-specific."[36]

The digital signature is the only form of electronic signature which satisfies all three of the UNCITRAL security evaluation factors, i.e., that an electronic signature should:

(1) authorize; (2) approve; and (3) protect against fraud.[37] 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.[38]

3.4 Disadvantages of the digital signature

The digital signature has at least two drawbacks. First, 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.[39]

The other disadvantage of the digital signature pertains to the certificate,[40] which must be issued by a Certification Authority ("CA").[41] Obtaining the certificate and 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.[42] 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.

[36] Id.

[37] Note 26 supra at 243.

[38] Note 26 supra at 252.

[39] Note 26 supra at 253.

[40] Under Croatian law, a certificate is defined as a "confirmation in electronic form which links the data for authentication of the electronic signature with a specific person and confirms the identity of such person." ESA, note 140 infra, art. 2(10).

[41] Under Croatian law, a CA is defined as "a legal or natural person who issues certificates or provides other services pertaining to electronic signatures." ESA, note 140 infra, art. 2(12). CA, the term used in Croatia and in this article, is used in most of the world's jurisdictions with the exception of the European Union, which uses "certification service provider." ESD, note 140 infra, art. 3.

[42] Note 26 supra at 253.

3.5 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 A (the sender) and B (the receiver) are attempting to consummate an online transaction, B needs an independent confirmation that A's message is actually from A before B can have faith that A's public key actually belongs to A. It is possible that an imposter could have sent B the public key, contending that it belongs to A when in fact it does not. 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.[43]

The most important job of the CA is to issue certificates which confirm basic facts about the subscriber, the subject of the digital certificate. The certificate is a digitized, computer-held record containing the most pertinent information about a transaction between two transacting parties: 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.[44] Sufficient information will be contained in the certificate to connect a public key to the particular subscriber.[45]

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.[46] 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.[47]

In order to indicate the authenticity of the digital certificate, the CA will sign it with his digital signature. Typically, 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 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.[48]

[43] Hogan (2000).

[44] Froomkin (1996).

[45] Note 43 supra at 425–426.

[46] Note 11 supra at 149.

[47] Note 11 supra at 150.

[48] Note 43 supra at 426–427.

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.[49] Nations around the world 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.[50]

A certificate is only as reputable as the CA that issues it. If the CA is unreliable and untrustworthy, the 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.[51]

4 Three generations of electronic signature law

4.1 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.[52] In the Utah statute, digital signatures were given legal recognition, but other types of electronic signatures were not.[53] 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 Armenia, Germany, India,[54] Italy, Malaysia, Nepal[55] and Russia.[56]

Unfortunately, these jurisdictions' choice of "technological-exclusivity" 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 disadvantages: more expense, lesser convenience, more complication and less adaptability to technologies used in other nations, or even by other persons within the same country.[57]

[49] Osty and Pulcanio (1999).

[50] See Berman (2001); and Maurushat (2005) arguing that multi-lateral recognition of CA's among China, Hong Kong and Singapore should only occur after their PKI legislation has been harmonized and each of them provides sufficient privacy protections for personal data.

[51] Hallerman (1999).

[52] State of Utah (1999).

[53] Id.

[54] Blythe (2006a).

[55] Blythe (2008).

[56] Note 27 supra at 234–237.

[57] It is debatable as to whether technological-neutrality or technological-specificity is the correct road to take. See Roland (2001).

4.2 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. Examples of permissive jurisdictions include the majority of states in the United States, the United Kingdom,[58] Australia and New Zealand.[59]

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.

4.3 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.[60] 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 a 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.[61]

[58] For concise coverage of American and British law, see Blythe (2005a).

[59] Note 27 supra at 234–237.

[60] United Nations (1996). See Blythe, Note 58 supra.

[61] Republic of Singapore (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

The moderate, hybrid position taken by Singapore has become the progressive trend in international electronic signature law and has been adopted in many jurisdictions, including these: Azerbaijan,[62] Barbados,[63] Bermuda,[64] China,[65] Dubai,[66] European Union,[67] Hong Kong,[68] Hungary,[69] Iran,[70] Japan,[71] Lithuania,[72] Pakistan,[73] South Korea,[74] Taiwan,[75] Tunisia[76] and Vanuatu.[77]

5 Computer laws of the European Union

Croatia, Macedonia and Turkey are "official candidate countries"[78] under serious consideration for admission to the European Union.[79] Accordingly, Croatia will eventually have to comply with the requirements imposed by the European Union's E-Signatures Directive and E-Commerce Directive, which are covered next.

5.1 E-Signatures Directive

The European Union enacted the E-Signatures Directive (hereinafter "ESD") on 13 December 1999.[80] The purposes of the ESD are to: promote the legal recognition of E-signatures; and create a legal framework for E-signatures and certification

Footnote 61 continued
electronic signature law established comprehensive rules for the licensing and regulation of Certification Authorities, whose critical role is to verify the of authenticity and integrity of electronic messages affixed to electronic signatures. Id. See Blythe (2007a).

[62] Blythe (2007b).

[63] Blythe (2007c).

[64] Note 32 supra at 234–37.

[65] Blythe (2007d).

[66] Blythe (2007e).

[67] Note 17 supra. See Blythe, Note 63 supra.

[68] Before amending its original digital signature law, Hong Kong only recognized digital signatures and was therefore a member of the First Wave. After amendments were made, Hong Kong joined the Third Wave. See Blythe (2005b).

[69] Blythe (2007f).

[70] Blythe (2006b).

[71] Blythe (2006c).

[72] Blythe (2007g).

[73] Blythe (2006d).

[74] Blythe (2006e).

[75] Blythe (2006f).

[76] Blythe (2006g).

[77] Blythe (2006h).

[78] Wikipedia. "European Union—Member States".

[79] For general information about the European Union, see U.S. Central Intelligence Agency ("CIA"), THE WORLD FACTBOOK, "European Union," 20 March 2008; https://www.cia.gov/library/publications/the-world-factbook/geos/ee.html.

[80] European Union (1999).

services, resulting in their greater use.[81] However, contract law and law relating to the use of documents are not the concern of the ESD.[82] The ESD contains definitions of a(n): E-signature;[83] advanced E-signature;[84] certification service provider ("CSP");[85] and certificate.[86]

5.1.1 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.[87] Furthermore, such an E-signature is admissible as evidence in a court of law.[88] 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 certificate was not issued by an accredited CSP; or the fact it was not generated with a secure signature-creation device.[89]

5.1.2 Certification service providers

The ESD refers to a certification authority ("CA") as a "certification service provider" ("CSP").[90] A CSP is not mandated to hold a license,[91] and is not required to be accredited.[92] Nevertheless, each Member State must regulate all of its CSP's

[81] ESD art. 1.

[82] ESD preamble 17 and art. 1.

[83] 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).

[84] 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).

[85] 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.

[86] 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).

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

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

[89] 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. See Arias (2007).

[90] As previously mentioned in note 41, the Croatian ESA uses the term "certification authority" instead of certification service provider. However, a CA and a CSP perform equivalent duties.

[91] 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.

[92] ESD preamble 12.

who issue qualified certificates.[93] These CSP's must meet more stringent qualifications than those which do not issue qualified certificates[94]; for example, they must use a secure signature-creation device[95] and must provide for secure signature verification.[96] 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.[97] 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 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.[98] 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.[99] A qualified certificate issued by a CSP in a non-EU nation

[93] 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.

[94] 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.

[95] 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.

[96] 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).

[97] ESD art. 4(1).

[98] 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).

[99] ESD art. 8.

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.[100]

5.1.3 E-signature Committee

An E-signature Committee ("Committee")[101] may be created to issue official standards for E-signature products.[102]

5.1.4 E-Government

Governments of the Member States should use E-signatures; if so, additional requirements may be imposed.[103] Specific governmental activities amenable to use of E-signatures include: purchasing, taxation, social security, health programs and the justice system.[104]

5.1.5 Implementation

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 signature-creation devices; and names and addresses of all accredited CSP's.[105] Each Member State was required to enact legislation necessary to accomplish the objectives of the ESD no later than 19 July 2001.[106] 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.[107]

[100] 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).

[101] 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).

[102] 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).

[103] 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.

[104] ESD preamble 19.

[105] ESD art. 11.

[106] ESD art. 13(1).

[107] ESD art. 12.

5.2 E-Commerce Directive

The European Union enacted the E-Commerce Directive (hereinafter "ECD") on 8 June 2000.[108] The ECD's purpose is to foster the free flow of E-commerce among the Member States.[109] 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.[110] 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."[111] The ECD refers to E-commerce as "information society services"[112] and refers to an E-commerce seller as a "service provider."[113] The ECD distinguishes a "recipient of the service"[114] and a "consumer."[115] Member States' laws pertinent to E-commerce or E-commerce service providers are referred to as "coordinated field."[116]

5.2.1 Member States' supervisory requirements

Each Member State is responsible for ensuring that domestically established service providers comply with the Member State's laws in the coordinated field.[117] A Member State may not use its laws in the coordinated field to restrict activities of

[108] European Union (2000).

[109] ECD art. 1(1).

[110] ECD art. 1(2).

[111] ECD preamble 11, 12, and 16; ECD art. 1(3)–(6).

[112] 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).

[113] 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).

[114] 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).

[115] 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).

[116] 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-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).

[117] ECD art. 3(1).

service providers established in other Member States.[118] The two aforementioned sentences are inapplicable in some specified situations.[119] Each Member State must ensure that a service provider, before commencing its activities, has complied with all legal requirements.[120]

5.2.2 *Service providers' requirements*

5.2.2.1 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.[121] Service providers are obliged to provide additional information in electronic advertisements.[122] Member States may allow unsolicited E-mail advertisements, but special rules apply to them.[123] Professional service providers using E-mail communiques must abide by the rules of their profession pertinent to "independence, dignity and honour of the profession,

[118] 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).

[119] 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 pertient 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.

[120] 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).

[121] 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).

[122] 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.

[123] 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.

professional secrecy and fairness toward clients and other members of the profession."[124]

5.2.3 E-contracts

Member States must recognize the legal validity of E-contracts and must avoid creation of obstacles to their creation or utilization.[125] Member States must ensure that service providers provide clear and comprehensive information to the customer before the order is placed.[126] After the customer's order has been placed, the seller must promptly acknowledge the receipt of the order using electronic communications.[127]

5.2.4 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[128]; cache[129]; or host.[130] Generally, an intermediary has no obligation to monitor the information.[131]

[124] 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).

[125] 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 5 years the Member State must justify to the Commission why it is necessary to maintain those exceptions. ECD art. 9(3).

[126] 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).

[127] 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).

[128] ECD art. 12.

[129] ECD art. 13.

[130] ECD art. 14.

[131] 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).

5.2.5 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.[132] Out-of-court settlement of E-commerce disputes is encouraged, and the ECD should not hamper Member States' informal dispute resolution procedures.[133] 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."[134] Member States are mandated to cooperate with one another in the implementation of the ECD.[135] Member States were mandated to enact all laws and regulations necessary for implementation of the ECD by 17 January 2002.[136] Those laws and regulations were required to include a list of sanctions applicable to violators.[137] 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."[138]

Member States are required to take all measures necessary to enforce their laws and regulations.[139]

6 Croatia's computer laws

6.1 Electronic Signature Act

Croatia enacted its Electronic Signature Act (hereinafter "ESA") in 2002.[140] The statute is to be implemented by the Minister of Economy ("Minister"),[141] and he is

[132] ECD preamble 49; ECD art. 16(1)(a) and 16(2).

[133] 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).

[134] ECD art. 18(1).

[135] 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. ECD preamble 61.

[136] ECD art. 22(1).

[137] ECD art. 20. The sanctions must be "effective, proportionate and dissuasive." Id.

[138] ECD preamble 63.

[139] ECD art. 20.

[140] Republic of Croatia (2002).

[141] ESA art. 7 and 36.

obliged to promulgate regulations to that effect.[142] The ESA distinguishes an E-signature and an advanced E-signature.[143] An advanced E-signature may be used as an alternative to a statutorily required handwritten signature or seal.[144] A Certification Authority ("CA")[145] issues a certificate[146] in order to confirm the identity of a subscriber.[147] A subscriber is responsible for giving accurate information to the CA and for provision of security over its private key and computer equipment.[148] The CA is responsible to check out the identity of a subscriber, to keep the information in the certificate up-to-date, to maintain an accurate register of issued certificates,[149] and to use a secure computer system.[150] A CA planning to go out of business must find a replacement CA, if possible.[151] The ESA contains ordinary rules for recognition of foreign CA's and the certificates they have issued.[152] It is a crime: to obtain unauthorized access to or use another's E-signature or private key; for a subscriber to fail to maintain security over the private key, or to fail to promptly inform the CA of a compromise of its security;

[142] ESA art. 42–44.

[143] The former is "a set of data in electronic form which are associated or logically connected with other data in electronic form and which serve to identify the signatory and the authenticity of the signed electronic document." ESA art. 2(1) and 3. The latter is an E-signature "which fully guarantees the identity of the signatory and which complies with the requirements stipulated in Article 4" of the ESA. ESA art. 2(2). Article 4 mandates that an advanced E-signature: be linked to the subscriber and no one else; conclusively indicate the subscriber; be generated with a tool under the exclusive control of the subscriber; and have a relationship with the attached so that any subsequent modification of the data is detectable. An advanced E-signature must be created with an advanced E-signature development tool possessing the most stringent security attributes. ESA art. 8 and 9.

[144] ESA art. 5. Ordinarily, an E-signature may not be contested merely because of its electronic form. However, there are exceptions; the following types of documents are mandated to be in paper form to be valid: real estate; probate; prenuptial agreements; encumberment of assets when a social welfare center must grant approval; living wills and ordinary wills; those requiring certification by a Notary Public; and others designated by another statute or regulations. ESA art. 6.

[145] A CA is required to have personnel with sufficient expertise, a sophisticated computer system, and other qualifications. ESA art. 12 and 17. These requirements must be reported to the Minister, along with its standard operating procedures. ESA art. 15. It is not compulsory for a CA to be licensed. ESA art. 14. However, all CA's must be "registered," i.e., the Minister must be informed of the qualifications if a CA plans to open a business; if qualified, the Minister will list the CA in its Directory of Registered CA's. ESA art. 16 and 21. Furthermore, if a CA desires accreditation by the Minister, it may apply for a license to be issued by the Minister verifying same; licensed CA's are referred to as "Qualified" CA's and are listed in the Minister's Directory of Qualified CA's. ESA art. 18 and 19. The Minister is empowered to conduct regular inspections of CA's. ESA art. 37 and 38.

[146] A certificate must contain specific types of information, including: the E-signature of the CA; the public key; and personal information of the subscriber. ESA art. 11.

[147] ESA art. 10 and 24.

[148] ESA art. 25–28.

[149] The CA's register of certificates should be shared with other CA's. ESA art. 34.

[150] ESA art. 29 and 32. CA's must promptly revoke a certificate at the request of the subscriber, and for other reasons. ESA art. 30. Certificates and supporting documentation must be stored for at least ten years after the issuance date.

[151] ESA art. 33.

[152] ESA art. 35.

and for a CA to fail to maintain proper security in reference to issuance of a certificate and the related register of certificates.[153]

6.2 Electronic Commerce Act

Croatia enacted its Electronic Commerce Act (hereinafter "ECA") in 2003.[154] E-commerce firms are not mandated to be licensed in Croatia, but must be registered with the Minister.[155] Commercial communications must be identified as such and, if unsolicited, can only be sent if the recipient has given prior approval.[156] An E-Contract is one "concluded fully or partially by natural or legal persons, sent, received, terminated, cancelled, joined, and shown in electronic manner by electronic, optical or similar means, including, but not limited to Internet transfer by legal or natural persons."[157] Ordinarily, an E-contract is legally valid.[158] An E-seller's offer must contain specific information[159]; an E-contract is not considered to have been consummated until the offeror receives notification of acceptance from the offeree. Customary rules pertinent to limited liability of Internet service providers are included in the ECA.[160] It is a crime for an E-seller to: refuse to give contact information; fail to give required information in a commercial communique; fail to allow the buyer access to the E-contract; and to submit to the regulator's demand for inspection.[161]

[153] ESA art. 39–41. The first two may be punished with a fine in the range of 2,000–10,000 HRK, and the last may be punished with a fine in the range of 5,000–100,000 HRK. Id.

[154] Republic of Croatia (2003). The statute is inapplicable to: data protection; taxation; Notaries Public; legal representation of a client in the court system; and to gambling. ECA art. 1(2). The ECA and other pertinent Croatian statutes apply to E-commerce firms located in Croatia, but are inapplicable to E-commerce firms located in other EU member states even if they intend to sell products via E-commerce in Croatia (except for transactions affecting copyright, E-money, real estate, insurance firms, consumer advertising, freedom of choice of law to govern a contract, and medical products. ECA art. 3 and 4.

[155] ECA art. 5. A specific list of information must be supplied by the E-commerce seller during registration. ECA art. 6.

[156] ECA art. 7 and 8.

[157] ECA art. 2(6).

[158] ECA art. 9(1)–(3). However, an E-contract cannot be used in these situations: prenuptial agreements; property agreements requiring authorization of a social welfare center; living wills and ordinary wills; donations; real estate transfers; Notaries Public; if another statute mandates the presence of a handwritten signature or certification of it; and surety agreements. ECA art. 9(4). A party's E-signature must be in compliance with the ESA. ECA art. 11.

[159] ECA art. 12. The E-contract generated must be capable of being printed, stored and retrieved by the buyer. ECA art. 13.

[160] ECA art. 16–21. The limitations concern caching, provision of links and dissemination of other party's materials over the internet. Id.

[161] ECA art. 23. The normal punishment is a fine in the range of 1,000 to 100,000 HRK; however, repeated or serious violations must result in a court order prohibiting the E-commerce activity for a period of 3–6 months. Id.

6.3 Electronic Document Act

Croatia enacted its Electronic Document Act (hereinafter "EDA") in 2005.[162] The EDA applies to private parties who have voluntarily agreed to use E-documents,[163] as well as government departments who have agreed to issue and accept E-documents.[164] An E-document must: be properly identified; indicate the name of its creator and recipient; indicate the time and place of transmission and reception; secure and incapable of unauthorized modification[165]; and accessible.[166] If a statute requires a document to be retained in its original form, that requirement will be deemed to have been met if it is kept as an E-document.[167] All copies of an E-document are deemed to be originals; if a document is prepared in both paper and electronic forms, they are deemed to be independent and neither is considered to be a copy of the other.[168,169] E-documents may be introduced as evidence in a court of law. The EDA contains ordinary rules pertinent to attribution[170] and time/place of transmission/receipt.[171] The following are crimes: tampering with the content or endorsements of an E-document[172]; refusing to accept an E-document after previously agreeing to do so; placing another party in an unfair position vis-à-vis the

[162] Republic of Croatia (2005).

[163] An E-document is defined as "the unambiguously connected integral set of data that have been electronically formed (prepared with the help of computers and other electronic devices), sent, received or stored on electronic, magnetic, optical or other medium, containing characteristics that determine the source (creator) and the authenticity of the contents and prove the integrity of contents in time," and their contents "include all forms of text in writing, data, pictures and drawings, maps, sound, music, speech." EDA art. 4(1). An E-document must be signed whenever it is transmitted and stored. EDA art. 15(2). The E-signature attached to an E-document must be an *advanced* E-signature as defined in the ESA. EDA art. 4(3).

[164] EDA art. 1 and 3. If the private parties or the government has agreed to use E-documents, they have the same legal validity as paper documents if all security requirements have been complied with. EDA art. 2 and 5.

[165] The computer system used with an E-document must use stringent security procedures. EDA art. 13(4).

[166] EDA art. 6 and 19(1). An E-document has two parts: the contents (with recipient's name) and the subscriber's E-signature with date and hour of generation. EDA art. 7. The internal and external form of an E-document must also be proper. EDA art. 8.

[167] EDA art. 20(1). However, appropriate security procedures must be in place to ensure that the document remains unaltered. EDA art. 20(2)-(3). Furthermore, the storage of the E-document may be entrusted to an agent if it uses appropriate security procedures. EDA art. 21–23.

[168] EDA art. 9. Verification of a paper printout of an E-document is to be done by a public authority within his scope of statutory authority; in all other cases, such verification must be performed by a Notary Public. EDA art. 10(2). Verified paper copies of an E-document have the same legal validity as the E-document. EDA art. 11(1).

[169] EDA art. 12(1). The amount of weight given the evidence depends on details pertinent to the E-document's "preparation, storage, transfer, safekeeping, authenticity and lack of change…" EDA art. 12(2).

[170] EDA art. 16.

[171] EDA art. 17–18.

[172] The maximum punishment is a fine of 60,000 HRK if the offense is committed on behalf of a legal entity. EDA art. 26(1). Additionally, a fine of 10,000 HRK or imprisonment for 15 days may be imposed upon a natural person responsible for the legal entity's action. EDA art. 26(2).

E-document's "exchange operations;" using a computer system in an E-commerce transaction that has insufficient personal data protection[173]; failure to respond to the sender's request for confirmation of receipt; improper use of E-documents; use of unsafe retention methods pertinent to E-documents; and failure to properly protect confidential data in E-documents.[174]

7 Recommendations for improvement of Croatia's computer laws

7.1 E-contract rules

Specific rules should be added to the ECA relating to attribution of an E-message, i.e., determination of when an E-message may be assumed to have emanated from a specific person. Furthermore, the existing rules pertinent to acknowledgement-of-receipt of an E-message are in need of revision. Any number of E-commerce laws could be used as a model; Barbados is but one example.[175]

7.2 Special rules for carriage contracts

Contracts for the delivery of goods—often referred to as "carriage" contracts—have unique nuances. Accordingly, special rules should be added to the ECA dealing with them. Croatia can look to the E-commerce law of Colombia[176] and Canada[177] for examples.

[173] The previous three crimes have a maximum punishment of 40,000 HRK if they are committed on behalf of a legal entity. EDA art. 27(1). Additionally, a fine of 5,000 HRK may be imposed upon a natural person responsible for the legal entity's action. EDA art. 27(2).

[174] The previous four crimes have a maximum punishment of 20,000 HRK if they are committed on behalf of a legal entity. EDA art. 28(1). Additionally, a fine of 3,000 HRK may be imposed upon a natural person responsible for the legal entity's action. EDA art. 28(2).

[175] Barbados (2001). See Blythe, Note 63 supra.

[176] Colombia's statute contains rules regarding these and other aspects of a carriage contract: (1) detailed description of the goods; (2) issuance of receipt; (3) confirmation of shipment; (4) notification of terms of the contract; (5) instructions to be conveyed to the transporter; (6) request of delivery of the goods; (7) authorization to deliver the goods; (7) buyer's notification of loss or damage of goods during transit; (8) seller's promise to deliver the goods to buyer or her agent; and (9) acquisition, waiver or transfer of rights in the agreement. In Colombia, E-documents may be used in the creation or implementation of carriage contracts, notwithstanding the fact that another statute may mandate the utilization of paper documents. This applies regardless of whether the statute creates a legal requirement, or provides for detrimental consequences if paper documents are not used. However, in order for E-documents to be used in the transfer of a right or obligation under a carriage contract, a "reliable method" must be employed to ensure the security and integrity of the message. Once data messages have begun to be used, paper documents are no longer valid. A party cannot revert to the use of paper documents until the other party has been informed that, henceforth, paper documents are to be used instead of data messages. Reversion to paper documents will not affect the rights of the parties which were created with E-documents. If a legal regulation exists in reference to paper documents relating to a carriage contract, that regulation will also be applied to a digital message used in lieu of paper documents. Republic of Colombia (1999).

[177] Uniform Law Conference of Canada (1999).

7.3 Consumer protections in E-contracts

Better consumer protections for E-commerce buyers need to be added to the ECA. As a model, Armenia can look to Tunisia's computer law[178]: (1) buyers have a "last chance" to review an order before it is entered into; (2) they have a 10-day window of opportunity to withdraw from an agreement after it has been made; (3) they have the right to a refund if the goods are late or if they do not conform to the specifications; and (4) the risk remains on the seller during the 10-day trial period after the goods have been received. Tunisian cyber-buyers enjoy some of the best protections in the world.[179]

7.4 Information technology courts

An adjudicator of E-commerce disputes often needs specialized knowledge. Accordingly, the ECA should establish Information Technology Courts as a court-of-first-instance for them. Each I.T. Court would be a tribunal with three experts: (1) the chairperson would be an attorney versed in E-commerce law; and the other persons would be (2) an I.T. expert and (3) a business management expert. The attorney would be required to hold a law degree and be a member of the bar with relevant legal experience; the I.T. person would be required to hold a graduate degree in an I.T.-related field and have experience in that field; and the business management expert would be required to hold a graduate degree in business administration and have managerial experience. The E-commerce law of the Kingdom of Nepal can be used as a model.[180]

7.5 Promote "cybersuites"

The governments of economically underdeveloped nations such as Croatia need to constantly be on the lookout for new sources of revenue. Accordingly, Croatia should consider the promotion of "cybersuites" *a la* the Republic of Vanuatu. Vanuatu enacted its E-Business Act ("EBA") to regulate E-commerce websites which have been rented by international business firms looking for a tax haven.[181]

[178] Republic of Tunisia (2000). See Stephen E. Blythe, Note 76 supra.

[179] Korea is one of the few nations that may offer better consumer protections than Tunisia. That country has enacted a separate statute specifically for E-commerce consumer protections—the E-Commerce Transactions Consumer Protection Act. See Republic of South Korea. Korean Legislation Research Institute, Act on the Consumer Protection in the Electronic Commerce Transactions (hereinafter "CPA"). 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. Furthermore, the CPA recently underwent a major overhaul with substantial amendments in Act No. 7487 of 31 March 2005; these amendments became effective on 1 April 2006. For a thorough analysis of the CPA, *see* Stephen E. Blythe, Note 74 supra. Iran also provides good consumer protections, including a window of opportunity to withdraw from an E-transaction previously entered into; however, the window in Iran is only seven days, as opposed to Tunisia's ten days. *See* Stephen E. Blythe, Note 70 supra.

[180] Kingdom of Nepal (2005). See Stephen E. Blythe, Note 55 supra.

[181] Republic of Vanuatu (2000). For a discussion of the E-Business Act by the Prime Minister of Vanuatu—the person who introduced the bill in Parliament—see Maautamate (Hon. Prime Minister) (2000). See also Stephen E. Blythe, Note 77 supra.

The EBA creates an Internet Free Trade Zone whereby individuals and firms can consummate E-commerce transactions while taking advantage of Vanuatu's low business income tax rates. Vanuatu-based websites—referred to as "cybersuites" in the EBA—are rented to foreign parties so that they may engage in E-commerce without the necessity of establishment of a formal international corporation with directors, shareholders and a registered office. Cybersuite proprietors are provided assistance in the creation of the website and its maintenance.[182] New cybersuite provisions should be added to the ECA.

7.6 Assert long-arm jurisdiction against foreign parties

Because so many of the E-commerce transactions incurred by the residents of Croatia will be with parties outside the borders of Croatia, it would be prudent for the ECA 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 Croatia.[183] Minimum contacts will exist, for example, if a cyber-seller outside of the country makes a sale to a person in Croatia. In that situation, the computer laws of Croatia should be applicable to the foreign party because that party has had an effect upon Croatia through the transmission of an electronic message that was received in Croatia. The foreign party should not be allowed to evade the jurisdiction of the Armenian courts merely because he is not physically present in the country. After all, E-commerce is an inherently multi-jurisdictional phenomenon.

8 Summary and conclusions

8.1 Computer law of the European Union

8.1.1 E-Signatures Directive

The ESD 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

[182] LOWTAX, p. 1.

[183] The Republic of Tonga is an example of a nation that has claimed long-arm jurisdiction over E-commerce parties, and its statute may be used as a model. *See* Stephen E. Blythe, Note 77 supra.

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.

8.1.2 E-Commerce Directive

The ECD's goal 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.

8.2 Computer law of Croatia

Croatia has enacted a comprehensive set of three computer laws. The ESA is third-generation and has the following remarkable attributes: detailed requirements for registration of CA's; a provision mandating CA's to share certificate-related information with other CA's; and a requirement that such information and pertinent documents be retained by a CA for a minimum of ten years after issuance of the certificate. The ECA's most noteworthy characteristics are: registration requirements for E-sellers; the mandate for an offeree to give confirmation of acceptance to an offeror before the E-contract is considered to be finalized; and the list of crimes applicable to E-sellers. The EDA's most distinguishing trait is its list of crimes pertinent to E-documents. All of the statutes suffer from a common weakness: there are too many exceptions from coverage.

8.3 Final thoughts: tweaking Croatia's ECL

Although it was an adequate first step, the ECL needs to be fine-tuned. The following modifications should be undertaken: (1) add E-contract attribution rules; (2) improve the E-contract acknowledgement-of-receipt rules; (3) add E-contract rules for carriage contracts; (4) strengthen the consumer protections of E-commerce buyers; (5) establish information technology courts; (6) add cybersuite provisions; and (7) add explicit long-arm jurisdiction.

References

American Bar Association. (2001). *PKI assessment guidelines*, V 0.30 at 301 (Public draft for comment no. 25); Retrieved from http://www.abanet.org/scitech/ec/isc/pagv30.pdf. Accessed 24 May 2008.

American Bar Association, Section of Science & Technology, Information Security Committee (1995, 1996). Electronic Commerce & Information Technology Division, Digital signature guidelines: Legal infrastructure for certification authorities and secure electronic commerce. *ABA Net*, p. 9; Retrieved from http://www.abanet.org/ftp/pub/scitech/ds-ms.doc. Accessed 24 May 2008.

Arias, M. L. (2007). Internet law—The EU law on electronic signatures and its recent report. *IBLS Internet Law—News Portal*, 3 December, p. 2; Retrieved http://www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1920. Accessed 10 February 2008.

Barbados. (2001). *Electronic Transactions Act*, CAP. 308B, 8 March, pp. s14–16; http://www.barbadosbusiness.gov.bb/miib/Legislation/Acts/investment_acts.cfm. Accessed 10 February 2008.

Berman, A. B. (2001). International divergence: the 'keys' to signing on the digital line—The cross-border recognition of electronic contracts and digital signatures. *Syracuse Journal of International Law and Commerce, 28*, 125, 143–144.

Blythe, S. E. (2005a). Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security. *Richmond Journal of Law and Technology, 11*(2), 6. Retrieved from http://law.richmond.edu/jolt/v11i2/article6.pdf and available at Lexis-Nexis: http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T3229558475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22_T3229558479&treeMax=true&treeWidth=0&csi=156342&docNo=7. Accessed 10 February 2008.

Blythe, S. E. (2005b). Electronic signature law and certification authority regulations of Hong Kong: Promoting E-commerce in the world's 'most wired' city. *North Carolina Journal of Law and Technology, 7*(1). Retrieved from http://www.jolt.unc.edu/currentissue.htm and available at Lexis-Nexis: http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T3229558475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22_T3229558479&treeMax=true&treeWidth=0&csi=241400&docNo=5. Accessed 10 February 2008.

Blythe, S. E. (2006a). A critique of India's information technology act and recommendations for improvement. *Syracuse Journal of International Law and Commerce, 34*, 1; Available at Lexis-Nexis: http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T3229558475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22_T3229558479&treeMax=true&treeWidth=0&csi=140728&docNo=3. Accessed 10 February 2008.

Blythe, S. E. (2006b). Tehran begins to digitize: Iran's E-Commerce law as a hopeful bridge to the world. *Sri Lanka Journal of International Law, 18*.

Blythe, S. E. (2006c). Cyber-law of Japan: Promoting E-commerce security, increasing personal information confidentiality and controlling computer access. *Journal of Internet Law,* New York, NY, USA: Aspen Publishers, Inc.; Retrieved from http://www.accessmylibrary.com/coms2/summary_0286-17306641_ITM. Accessed 10 February 2008.

Blythe, S. E. (2006d). Pakistan goes digital: The electronic transactions ordinance as a facilitator of growth for E-commerce. *Journal of Islamic State Practices in international Law, 2*, 2. Retrieved from: http://electronicpublications.org/catalogue.php?id=46. Accessed 10 February 2008.

Blythe, S. E. (2006e). The tiger on the Peninsula is digitized: Korean E-commerce law as a driving force in the world's most computer-savvy nation. *Houston Journal oF International Law, 28*(3), 573.

Blythe, S. E. (2006f). Taiwan's Electronic Signature Act: Facilitating the E-commerce boom with enhanced security. In *Proceedings of the Sixth Annual Hawaii International Conference on Business*, Honolulu, Hawaii, USA, May 25–28. Retrieved from: http://www.hicbusiness.org/Proceedings_Bus.htm. Accessed 10 February 2008.

Blythe, S. E. (2006g). Computer law of Tunisia: Promoting secure E-commerce transactions with electronic signatures. *Arab Law Journal, 20*, 240–267. Retrieved from: http://www.ingentaconnect.com/content/brill/alq. Accessed 10 February 2008.

Blythe, S. E. (2006h). South pacific computer law: Promoting E-commerce in Vanuatu and fighting cyber-crime in Tonga. *Journal of South Pacific Law, 10*(1). Retrieved from: http://www.paclii.org/journals/fJSPL/vol10/2.shtml. Accessed 10 February 2008.

Blythe, S. E. (2007a). Singapore computer law: An international trend-setter with a moderate degree of technological neutrality. *Ohio Northern University Law Review, 33*(2), 525–562; Available at Lexis-Nexis: http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T3229558475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_

T3229558480&cisb=22_T3229558479&treeMax=true&treeWidth=0&csi=140724&docNo=1. Accessed 10 February 2008.

Blythe, S. E. (2007b). Azerbaijan's E-commerce statutes: Contributing to economic growth and globalization in the Caucasus Region. *Columbia Journal of East European Law, 1*(1), 44–75.

Blythe, S. E. (2007c). The Barbados Electronic Transactions Act: A comparison with the U.S. model statute. *Caribbean Law Review, 16*.

Blythe, S. E. (2007d). China's new electronic signature law and certification authority regulations: A catalyst for dramatic future growth of E-commerce. *Chicago-Kent Journal of Intellectual Property, 7*, 1. Retrieved from http://jip.kentlaw.edu/currentissue.asp and at Lexis-Nexis: http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T3229558475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22_T3229558479&treeMax=true&treeWidth=0&csi=221052&docNo=2. Accessed 10 February 2008.

Blythe, S. E. (2007e). The Dubai electronic transactions statute: A prototype for E-commerce law in the United Arab Emirates and the G.C.C. countries. *Journal of Economics and Administrative Sciences, 23*, 1; Retrieved from http://jeas.cbe.uaeu.ac.ae/. Accessed 10 February 2008.

Blythe, S. E. (2007f). Hungary's Electronic Signature Act: Enhancing economic development with secure E-commerce transactions. *Information and Communications Technology Law, 15*(47); http://www.tandf.co.uk/journals/journal.asp?issn=1360-0834&linktype=5. Accessed 10 February 2008.

Blythe, S. E. (2007g). Lithuania's electronic signature law: Providing more security in E-commerce transactions. *Barry Law Review, 8*, 23. Available at Lexis-Nexis: http://www.lexisnexis.com.eproxy3.lib.hku.hk/us/lnacademic/results/docview/docview.do?risb=21_T3229558475&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T3229558480&cisb=22_T3229558479&treeMax=true&treeWidth=0&csi=254558&docNo=6. Accessed 10 February 2008.

Blythe, S. E. (2008). On top of the world, and wired: A critique of Nepal's E-Commerce Law. *Journal of High Technology Law, 8*(2), forthcoming

Chung, R. C. Y. (2003). Hong Kong's 'smart' identity card: Data privacy issues and implications for a post-September 11th America. *Asian-Pacific Law and Policy Journal, 4*, 442.

CYBER-SIGN. *The legality of electronic signatures using cyber-sign is well established*. Retrieved from http://www.cybersign.com/news_news.htm. Accessed 10 February 2008.

Dessent, M. (2002). Browse-Wraps, Click-Wraps and Cyberlaw: Our shrinking (Wrap) world. *Thomas Jefferson Law Review, 25*(1), 4.

European Union. (1999). Directive 1999/93/EC of the European Parliament and of the council of 13 December 1999 on a community framework for electronic signatures. *Official Journal L*, 013, 19/01/2000, pp. 12–20 (often referred to as "E-Signatures Directive"); Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML. Accessed 10 February 2008.

European Union. (2000). 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. *The Internal Market*, *Official Journal, 178*, 17/07/2000, pp. 1–16 (often referred to as "E-Commerce Directive"); Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML. Accessed 10 February 2008.

Fischer, S. F. (2001). 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. *Boston University Journal of Science and Technology Law, 7*, 229, 233.

Froomkin, A. M. (1996). The essential role of trusted third parties in Electronic Commerce. *Oregon Law Review, 75*, 49, 58.

Hallerman, D. (1999). Will banks become E-commerce authorities? *Bank Technology News, 12*, June 1.

Hogan, T. C. (2000). Notes and comments—technology, "Now that the floodgates have been opened, why haven't banks rushed into the certification authority business? *North Carolina Banking Institute, 4*, 417, 424–425.

LOWTAX. "Vanuatu E-commerce," p. 1; http://www.lowtax.net/lowtax/html/jvaecom.html. Accessed 10 February 2008.

Kingdom of Nepal. (2005). Electronic transactions ordinance no. 32 of the year 2061 B.S. (2005 A.D.), s60–71. The original version, in Nepalese Language, is available at the website of the Nepal Telecommunications Authority: Retrieved from http://www.nta.gov.np/cyber_law.html. 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: Retrieved from http://www.hlcit.gov.np/pdf/englishcyberlaw.pdf. Accessed 10 February 2008.

Maautamate, B. T. S. (Hon. Prime Minister) MP, Government of the Republic of Vanuatu (2000) 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. 8–10; Retrieved from http://www.vanuatugovernment.gov.vu/government/library/Exp%20note%20ecommerce%20acts.doc. Accessed 10 February 2008.

Maurushat, A. (2005). Multi-lateral recognition of PKI certification authorities in the Asian region: Transborder data flow and information privacy issues. *Hong Kong Law Journal, 35*(3), 569.

United Nations. (1996). United Nations Commission on International Trade Law ("UNCITRAL"), Model law on electronic commerce with guide to enactment ("MLEC"), G.A. Res. 51/162, U.N. GAOR, 51st Sess., Supp. No. 49, at 336, U.N. Doc. A/51/49; Retrieved from http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm. Accessed 10 February 2008.

Osty, M. J., & Pulcanio, M. J. (1999). The liability of certification authorities to relying third parties. *John Marshall Journal of Computer and Information Law, 17*, 961.

Poggi, C. T. (2000). Electronic commerce legislation: An analysis of European and American approaches to contract formation. *Virginia Journal of International Law, 41*, 224, 250–251.

Pun, K. H., Lucas Hui, K. P. Chow, W. W. Tsang, C. F. Chong, & Chan, H. W. (2002). Review of the electronic transactions ordinance: can the personal identification number replace the digital signature? *Hong Kong Law Journal, 32*, 241, 256.

Hong Kong Special Autonomous Region. (2000). *Electronic Transactions Ordinance*, Ord. No. 1 of 2000, s2.

Republic of Colombia. (1999). *Law regulating data messages, electronic trade, digital signatures and certification entities* (13 January), art. 26 and 27, Official Translation No. 7 by Maria del Pilar Mejia de Restrepo; Retrieved from http://www.qmw.ac.uk/~t16345/colombia_en_final.htm. Accessed 10 February 2008.

Republic of Croatia. (2002). Electronic Signature Act, 17 January; Retrieved from http://www.apiu.hr/docs/apiuEN/documents/84/Original.pdf. Accessed 10 February 2008.

Republic of Croatia. (2003). *Electronic Commerce Act*, 15 October; Retrieved from http://www.georges-chatillon.eu/IMG/rtf/2003_21_10_Loi_Commerce_electronique_Croatie.rtf. Accessed 10 February 2008.

Republic of Croatia. (2005). *Electronic Document Act ("EDA")*, 9 December; Retrieved from http://www.ehrvatska.hr/sdu/en/Zakonodavstvo/RH/categoryParagraph/07/document/eDocument_Act.pdf. Accessed 10 February 2008.

Republic of Singapore. (1998). *Electronic Transactions Act* (Cap. 88), 10 July; Retrieved from http://agcvldb4.agc.gov.sg/. Accessed 10 February 2008.

Republic of South Korea. (2002). Act on the consumer protection in the electronic commerce transactions. *Statutes of The Republic of Korea, 13*, pp. 481 to 485–430 (English translation by Korean Legislation Research Institute).

Republic of Tunisia. (2000). Electronic exchanges and electronic commerce law; http://www.bakernet.com.org. Accessed 10 February 2008.

Republic of Vanuatu. (2000). E-business ACT (Act no. 25 of 2000), Preamble; Retrieved from http://www.paclii.org/cgi-paclii/disp.pl/vu/legis/num%5fact/ea2000125.html. Accessed 10 February 2008.

Roland, S. E. (2001). The uniform electronic signatures in Global and National Commerce Act: Removing barriers to E-commerce or just replacing them with privacy and security issues? *Suffolk University Law Review, 35*, 625, 638–645.

Smedinghoff, T. J. (1999). Electronic contracts: An overview of law and legislation. 564 Practising Law Institute: Patents handbook series at 125, 162.

State of Utah. (1999). Utah code annotated 46–3–101 *et seq.*

Stern, J. E. (2001). Federal legislation: The electronic signatures in Global and National Commerce Act. *Berkeley Technology Law Journal, 16*, 391, 395 (2001).

Tang, D. K. Y., & Weinstein, C. G. (1999). Electronic contracting: American and international proposals for legal structures. In M. Chrisopher (Ed.), *Regulation and deregulation: Policy and practice in the utilities and financial services industries.* (pp. 321, 333). Oxford: Oxford University Press.

Uniform Law Conference of Canada, *Uniform Electronic Commerce Act*. (1999), ss24–ss25; Retrieved from http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1&print=1. Accessed 10 February 2008.

United States of America. (1998). Uniform Commercial Code ss 2–201 and 2–209.

United States of America. (2008). Central intelligence agency ("CIA"), *The World Factbook*, "Croatia," 20 March 2008, p. 1; Retrieved from http://www.cia.gov/library/publications/the-world-factbook/print/hr.html. Accessed 10 February 2008.

Wright, B. (2001). Symposium: Cyber rights, protection, and markets: Article, 'Eggs in baskets: Distributing the risks of electronic signatures'. *West Los Angeles Law Review, 32*, 215, 225–226.

Wikipedia. "European Union—Member States"; http://en.wikipedia.org/wiki/European_union. Accessed 10 February 2008.

Zaremba, J. (2003). International electronic transaction contracts between U.S. and E.U. companies and customers. *Connecticut Journal of International Law, 18*, 479, 512 (2003).