

**The Dubai Electronic Transactions Statute: A Prototype for
E-Commerce Law in the United Arab Emirates and the G. C. C. Countries**

**Dr. Stephen E. Blythe
Ph. D. Candidate in Law
University of Hong Kong
Hong Kong - China**

Abstract

Dubai's Electronic Transactions Law ("ETL") is designed to stimulate E-commerce in the emirate by improving the authenticity and integrity of electronic transactions. The ETL recognizes the legal validity of electronic documents and electronic signatures as acceptable substitutes for paper documents and ink signatures, respectively. Accordingly, electronic records may be used to comply with a statutory writing requirement, original document requirement and retention requirement, and an electronic signature attached to an electronic document may be used to comply with a statutory requirement for a paper-and-ink signature. If all parties are in agreement, a contract may be in electronic form and is just as legally enforceable as a written one. The ETL does not mandate Dubai's governmental agencies to utilize electronic documents, but they may elect to do so. The ETL has created a compulsory system of licensing of Certification Authorities ("CA"). Their role is to ascertain the identity of a subscriber and to attest in an issued Certificate that the electronic signature used by that subscriber belongs to him. The ETL contains a list of computer crimes. The statute establishes a sound framework for E-commerce, but it could be improved by adding consumer protections, more computer crimes, mandatory E-government, I.T. courts and long-arm jurisdiction. The ETL's exclusion of wills should be eliminated.

Objectives of the Article

The objectives of this article are to: (1) introduce the reader to the United Arab Emirates and to Dubai's preeminence in high technology in the Middle East; (2) explain the role of electronic signatures, cryptology, public key infrastructure, and Certification Authorities; (3) analyze Dubai's Electronic Transactions Law; and (4) make recommendations for improvement of the Dubai law.

The United Arab Emirates

The United Arab Emirates ("UAE") is on the southern coast of the Arabian Gulf and is tucked between Saudi Arabia and Oman. The area now comprising the UAE was once controlled by seven independent emirates:

Abu Dhabi, Dubai, Sharjah, Ajman, Umm Al-Qaiwain, Fujairah and Ras Al-Khaimah. In 1971, six of the emirates merged to create the UAE, and the seventh (Ras Al-Khaimah) joined them in 1972 (CIA 2006, p. 1). At that time, the emirates were quite poor and one purpose of their union was to become more economically viable. They succeeded! Over the next several decades, the wealth of the UAE dramatically escalated with the discovery of almost 10% of the world's proven oil reserves and one-fourth of the world's proven natural gas reserves (USTR 2005). In 2005, UAE's Gross Domestic Product ("GDP") was estimated to be \$74.51 billion, with GDP per capita a gigantic \$29,100. The growth of the UAE's economy has been strengthened by access to a plentiful supply of cheap labor coming from Pakistan, India, other south Asian countries, and east African nations. In fact, almost 74% of the working-age (15 to 64 years) population is non-national (CIA 2006, p. 7).

Dubai Preeminence in High Technology in the Middle East

Abu Dhabi is the capital city of the UAE. However, Dubai is the commercial centre not only of the UAE, but of the entire Middle East. The Ruler of Dubai is H.H. Mohammed bin Rashid al Maktoum, who assumed his position when his brother died suddenly on 5 January 2006 (CIA 2006, p. 5). While Crown Prince, Sheikh Mohammed exhibited vision and foresight in his realization of the critical importance that information technology would play in the economic development of Dubai, the UAE and the Arab World. H.H. established his own website (located at <http://www.sheikhmohammed.co.ae>) to be used as a direct means of communication with the citizens of Dubai. By 2001, E-government had begun to be implemented in the emirate (Mathia 2000). In 2002, Sheikh Mohammed established the Dubai Technology, Electronic Commerce and Media Free Zone, often referred to as "Dubai Internet City." Dubai Internet City is conceptually similar to the "Cyberport" of Hong Kong. The idea is to place many I.T. firms in close proximity in order for them to achieve synergy. By 2005, Dubai Internet City had become home to over 650 high-tech firms employing more than 14,000 workers (CPILive.Net 2005).

Dubai's E-commerce law was enacted as a companion statute to the one which created Dubai Internet City (Khaleej Times 2002). Sheikh Mohammed has recently taken the initiative toward achievement of a uniform federal E-commerce law for the entire UAE; it is currently being developed, and the federal statute is expected to be similar to that of the Emirate of Dubai (AGIP Bulletin 2005). Furthermore, H.H. wants to work toward a uniform E-commerce law for all six of the Gulf Cooperation Council (see GCC) nations. In November 20-21, 2005, Sheikh Mohammed

convened a conference in Abu Dhabi with representatives from all of the G.C.C. nations. The purpose of the conference was to lay the groundwork for a common E-commerce law in the region. H.H. made the keynote speech at the conference. Other speakers included Shaikha Lubna Al Qasimi, Minister of Economy and Planning of the UAE, and Hamad Abdul Rahman Al Attiya, Secretary-General of the GCC (ITP Technology 2005). In all likelihood, given the leadership that Sheikh Mohammed has already exhibited in I.T. development, the Dubai E-commerce law will eventually serve as a prototype for the uniform E-commerce law expected to emerge in the G.C.C. That is why Dubai's E-commerce law deserves to be studied and is the focus of this article. In his review of the literature of Dubai E-commerce law, the author uncovered only one journal article (Qudah 2002). It is only four pages in length and does not sufficiently cover the subject matter.

Electronic Signature

Contract law worldwide has traditionally required the parties to affix their signatures to a document (e.g., UCC 1998). 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," (Smedinghoff 1999) 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." (EU Directive 1999) An electronic signature may take a number of forms: a digital signature, a digitized fingerprint, a retinal scan, a pin number, a digitized image of a handwritten signature that is attached to an electronic message, or merely a name typed at the end of an e-mail message (Tang 1999).

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 (Dessent 2002)." This statement seems to assume that all E-signatures offer an equal degree of security. However, such an assumption would be erroneous; some electronic signatures offer more security than others. It is prudent for E-commerce participants to use the more secure types of electronic signatures, notwithstanding their greater degree of complexity and expense.

Online Contracts: Four Levels of Security

When entering into a contract online, four degrees of security are possible (Stern 2001).

1. The first level would exist if a party accepted an offer by merely clicking an “I Agree” button on a computer screen.
2. The second level of security would be incurred if secrets were shared between the two contracting parties. This would be exemplified by the use of a password or a credit card number to verify a customer’s intention that goods or services were to be purchased.
3. The third level is achieved with biometrics. Biometric methods involve a unique physical attribute of the contracting party, and these are inherently extremely difficult to replicate by a would-be cyber-thief. Examples include: a voice pattern, face recognition, a scan of the retina or the iris within one’s eyeball, a digital reproduction of a fingerprint (Chung 2003), 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. 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” (Stern 2001) during signing would be recorded, and this information is almost impossible to duplicate by an imposter. Biometrics, despite its potential utility as a form of electronic signature, has at least two drawbacks in comparison with the digital signature: (1) The attachment of a person’s biological traits to a document does not ensure that the document has not been altered, i.e., it “does not freeze the contents of the document;” 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 (Pun 2002). The digital signature does not have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers. This view is not shared by all, however (e.g., Wright 2001). Many also recommend the use of both methods; this was the course taken by the Hong Kong government in designing its identity card (Chung 2003).
4. The digital signature is considered the fourth level because it is more complex than biometrics. Many laypersons erroneously assume that the digital signature is merely a digitized version of a handwritten signature. This is not the case, however; the digital signature refers to the entire document. 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 (Smedinghoff 1999).” 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 (Poggi 2000).

Digital Signature Technology: Public Key Infrastructure

The technology used with digital signatures is known as Public Key Infrastructure, or “PKI” (Fischer 2001). PKI consists of four steps:

1. The first step in utilizing this technology is to create a public-private key pair; the private key will be kept in confidence by the sender, but the public key will be available online (ABA PKI Assessment Guidelines 2001).
2. The second step is for the sender to digitally “sign” the message by creating a unique digest of the message and encrypting it. A “hash value” is created by applying a “hash function”—a standard mathematical function—to the contents of the electronic document. The hash value, ordinarily consisting of a sequence of 160 bits, is a digest of the document’s contents. Whereupon, the hash function is encrypted, or scrambled, by the signatory using his private key. The encrypted hash function is the “digital signature” for the document (Poggi 2001).
3. The third step is to attach the digital signature to the message and to send both to the recipient.
4. The fourth step is for the recipient to decrypt the digital signature by using the sender’s public key. If decryption is possible the recipient knows the message is authentic, i.e., that it came from the purported sender. Finally, the recipient will create a second message digest of the communication and compare it to the decrypted message digest (ABA Digital Signature Guidelines 1995). If they match, the recipient knows the message has not been altered (Zaremba 2003).

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.” Although a handwritten signature is only “signatory-specific,” the digital signature is both “signatory-specific” and “document-specific” (Poggi 2000).

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

electronic signature should: (1) authorize; (2) approve; and (3) protect against fraud. 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 (Poggi 2000).

Disadvantages of the Digital Signature

The digital signature has at least two drawbacks. Firstly, since the private key of each person is rather difficult to memorize, they are most often stored in computers. If the computer is not kept in a secure location, the contents of the private key may be vulnerable. This heightens the necessity of maintaining the security of the private key and protecting it from intruders. However, it should be noted that this weakness of the digital signature is also common to most other forms of electronic signatures. The password or the PIN faces similar security problems. Therefore, with good security policies and procedures, this disadvantage can be minimized (Poggi 2000).

The other disadvantage of the digital signature pertains to the digital certificate, which must be issued by a Certification Authority (“CA”). 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 (Poggi 2000). Because the CA plays such a vital role in the viability of the digital signature, it is essential for the user to understand exactly what the CA does.

The Critical Role of the Certification Authority

In order for PKI to realize its potential, it is crucial that the user be able to ensure the authenticity of the public key (available online) used to verify the digital signature. If 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 (Hogan 2000).

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 (Froomkin 1996). Sufficient information will be contained in the certificate to connect a public key to the particular subscriber (Hogan 2000).

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. 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 (Smedinghoff 1999).

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 (Hogan 2000).

One of the recurring problems for digital signature lawmakers is in trying to fairly apportion the liability for risk of computer fraud between the CA and the subscriber. Nations around the world 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 (Berman 2001).

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 (Hallerman 1999).

Electronic Signature Laws

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. In the Utah statute, digital signatures were given legal recognition, but other types of electronic signatures were not (UCA 1995). 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 Germany, Italy, Malaysia and Russia (Fischer 2001).

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 (Roland 2001).

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, Australia and New Zealand (Fischer 2001).

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 (Blythe #1 2005).

The Third Wave:**Moderate Degree of Technological Neutrality**

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 (UN 1996). 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 (Singapore 1998).

Four years later, Dubai joined the Third Wave by emulating the hybrid perspective of Singapore. This moderate position has now become the progressive trend in international electronic signature law. The hybrid approach is also the one taken by the European Union's E-Signatures Directive (EU Directive 1999), Bermuda (Fischer 2001), Pakistan (Blythe #2 2006), Azerbaijan (Blythe #3 2006) and most recently, China (Zhang & Lingfei 2005).

Dubai's Electronic Transactions Law**Purposes**

Dubai's Law of Electronic Transactions and Commerce No. 2/2002 (Dubai 2002) (hereinafter "Electronic Transactions Law" or "ETL") was enacted on 12 February 2002 and went into effect a short time later after publication in the Gazette (Dubai 2002, art. 39). Its purposes are to: (1) attain a greater degree of reliability in electronic records and thereby improve electronic communication (Dubai 2002, art. 3(1)); (2) establish standards regarding electronic records and electronic signatures and thereby promote the development of the business and legal framework necessary for attainment of security in electronic transactions (Dubai 2002, art. 3(2)); (3) encourage government agencies to begin to utilize electronic records and signatures and to begin to accept citizens' filing of electronic records and

signatures in order to attain the efficiencies offered by an effective system of E-Government (Dubai 2002, art. 3(3)); (4) reduce fraud in E-commerce by creating a framework which makes it more difficult to commit forgery of an E-signature (Dubai 2002, art. 3(4)); (5) attain the maximum possible degree of authentication and integrity in electronic transactions by creation of uniform standards, rules and regulations (Dubai 2002, art. 3(5)); (6) facilitate the attainment of confidence of the general public in the authenticity and accuracy of electronic transactions, electronic records and electronic communications (Dubai 2002, art. 3(6)); and (7) encourage the utilization of electronic signatures in electronic transactions and thereby promote the development of E-commerce at both national and international levels (Dubai 2002, art. 3(7)).

Implementation

The Chairman Has Great Discretion

One of the distinguishing characteristics of the Dubai law is the high degree of discretion given to the Chairman. The author is presently pursuing a multi-year study of international E-commerce law, and this is the first instance he has encountered such a high degree of implementation authority invested in one person. This is not a criticism; this is merely an observation. The Chairman is the primary implementer of the ETL and is granted a great deal of decision-making power in that regard. For example, the

Chairman: (1) creates and enforces regulations in order to implement the ETL (Dubai 2002, art. 38); (2) appoints the Commissioner of Certification Authorities (Dubai 2002, art. 23); (3) may exempt any person, organization or body from the provisions of the ETL or its implementation regulations whenever “he thinks fit” (Dubai 2002, art. 36); (4) may establish and employ special courts or arbitration tribunals to deal with lawsuits and disputes arising from the ETL (Dubai 2002, art. 37); and (5) may declare, at his discretion, that certain types of cases are not subject to the requirements imposed by ETL articles 15, 16 and 17 (Dubai 2002, art. 18).

E-Government

The ETL does not mandate any agency of the government to accept or to issue electronic documents; however, it is “permissible” for any agency to do so (Dubai 2002, art. 27(1)). Specifically, government agencies may do the following: (1) accept E-documents to comply with a citizen’s filing requirement; (2) allow E-documents to be used to comply with a citizen’s requirement to create or to retain a document (Dubai 2002, art. 27(1)(a)); (3) issue individuals’ licenses or permits in E-document form; (4) issue notices of government decisions or approvals in E-document form (Dubai 2002, art.

27(1)(b)); (5) accept citizens' payment of fees in electronic form (Dubai 2002, art. 27(1)(c)); and (6) issue tenders for bids pertaining to government purchases, and accept related bids, in E-document form (Dubai 2002, art. 27(1)(d)).

If a government agency engages in any of the aforementioned forms of E-government, it may specify: (1) the format of the electronic record; (2) the method of creation, filing, retention, submission or issuance of the electronic record (Dubai 2002, art. 27(2)(a)); (3) the format, method of submission and procedures pertaining to government tenders; (4) the format, method of reception and procedures pertaining to the receiving of bids; (5) the format, method used and procedures pertaining to government purchases (Dubai 2002, art. 27(2)(b)); (6) the type of Electronic Signature required to be used (Dubai 2002, art. 27(2)(c)); (7) the format and the method in which the Electronic Signature will be attached to the E-document; (8) the criteria required to be met by a CA whenever a CA is used to store E-documents (Dubai 2002, art. 27(2)(d)); (9) the security procedures to be followed in order to preserve the integrity of E-documents or E-payments (Dubai 2002, art. 27(2)(f); and (10) other conditions or rules pertinent to the transmission of paper documents, if paper documents are used to confirm E-payments (Dubai 2002, art. 27(2)(g)).

Exceptions: ETL Inapplicable in Some Situations

Electronic documents are unacceptable as: (1) wills and other documents of testamentary disposition; (2) marriage certificates; (3) divorce decrees (Dubai 2002, art 5(1)(i)); (4) real property deeds (Dubai 2002, art. 5(1)(ii)); (5) contracts pertaining to the sale or purchase of real property; (6) contracts to lease real property for more than ten years, and documents associated with rights in those leases (Dubai 2002, art. 5(1)(iv)); (7) negotiable instruments (Dubai 2002, art. 5(1)(iii)) and (8) any document legally required to be notarized (Dubai 2002, art. 5(1)(v)).

The Chairman, by issuance of an order, is authorized to add to, delete from or modify the list of exceptions in the preceding paragraph (Dubai 2002, art. 5(2)).

Legal Recognition of Electronic Records

Mere Fact of Electronic Form Insufficient to Avoid Recognition

No denial of legal recognition, admissibility or enforceability will be allowed based on the mere fact that a communication or record is in electronic form (Dubai 2002, art. 7(1)). If a communiqué refers to specific information, but does not include the information, it will nevertheless be

enforceable so long as the information is retrievable and the communiqué states how it can be retrieved (Dubai 2002, art. 7(2)).

Electronic Records Can Comply With Retention Requirement

If electronic records are mandated by law to be stored, that mandate will be complied with by the storage of records in electronic form, provided: (1) the information is accessible and can be stored for reference at a later date (Dubai 2002, art. 8(1)(b)); (2) the format used in the electronic form is identical to the one in which it was “generated, sent or received,” or the format is a correct depiction of that information (Dubai 2002, art. 8(1)(a)); and (3) the location and date of the transmission and reception is also stored (Dubai 2002, art. 8(1)(c)). The electronic records may be in the custody of the principal’s agent (Dubai 2002, art. 8(3)).

There is no obligation to retain information which is automatically generated by a computer information system during the process of sending or receiving a communiqué (Dubai 2002, art. 8(2)).

This provision does not affect other statutes which may have more stringent retention requirements, e.g.: (1) usage of a specific type of computer information system; (2) adherence to specific procedures; or (3) retention by a specified agent (Dubai 2002, art. 8(4)).

Electronic Records Can Comply With Requirement To Be “In Writing”

If a law or statute requires information to be in writing to be recognized, or characterizes information as mandated to be in written form, the electronic form will suffice if: (1) it is in the same format as the original or is an accurate depiction of the information contained in the original; (2) it can be retrieved for use at a later time; and (3) the origin and destination of a communiqué, and its dates of transmission and reception, are stored (Dubai 2002, art. 9)).

Electronic Signature Can Comply With Signature Requirement

If a law mandates the affixation of a person’s signature on a paper document (or for adverse consequences in the absence of a signature), this requirement will be met with an electronic signature affixed to an electronic record, provided: (1) a reliable method of identification of the person is used; (2) reliable evidence shows that the person intended to sign or otherwise adopt the information of the electronic record to which the electronic signature is affixed (Dubai 2002, art. 10(1)); and (3) it is reasonable to rely on the electronic signature (Dubai 2002, art. 21(1)).

Electronic signatures which are supported by a Certificate issued by an accredited CA will ordinarily comply with a statutory requirement for a signature on a paper document; reliance on them is presumed to be reasonable (Dubai 2002, art. 20)). Nevertheless, the relying party bears the burden of taking “reasonable and necessary steps” to confirm the validity of the Certificate and that it has not been suspended or revoked (Dubai 2002, art. 21(2)).

However, an electronic signature meeting the reasonableness requirement will not be refused legal recognition merely because it is not supported by a Certificate. Factors to be considered in the determination of whether the reliance was reasonable include: (1) the type of transaction; (2) the monetary value or importance of the transaction; (3) whether the relying party took appropriate steps to confirm the signatory’s identity, (4) whether the electronic signature was supported by a Certificate, and the status of the Certificate; (5) course of dealing or trade usage between the two parties; and (6) any other relevant factors (Dubai 2002, art. 21(3)). If in light of all of these factors the reasonableness test is not met, then the relying party assumes the legal risk that the electronic signature is invalid (Dubai 2002, art. 21(4)).

Electronic Records Can Comply With Original Requirement

If a law mandates that an original paper document must be presented in order to meet a legal requirement, or if a law requires that a paper document must be stored in its original form, that mandate is met if: (1) there is a “technically reliable assurance” that the electronic document, from the time of its creation until the present, has not been altered; and (2) if required to be presented, the information contained in the electronic record is readily retrievable and will be an accurate representation of the original (Dubai 2002, art. 11)).

Admissibility of Electronic Records and Evidential Weight Granted to Them

In a court of law, the rules of evidence shall not be construed in a manner that will refuse to admit an electronic record or electronic signature into evidence: (1) merely because of its electronic form; or (2) merely because it is not in its original form, so long as it is the “best evidence” available (Dubai 2002, art. 12(1)).

Factors to consider in determination of the evidential weight to be given an electronic record include: (1) the degree of trust and reliance that can be given the electronic record, taking into account the means of generation,

storage and communication; (2) whether the electronic record's integrity has been maintained since it was created, i.e., the trustworthiness of the record and whether there is assurance that it has not been altered; (3) the reliability of the sender and the means of identification of the sender; and (4) other relevant factors (Dubai 2002, art. 12(2)).

Through application of authentication procedures agreed to by the parties, it can be verified that, at the time of its creation, a Protected Electronic Signature: (1) was unique to that person; (2) confirmed the identity of the person; (3) was under the person's control; and (4) was linked to the electronic record so that there is reliance assurance of the signature's integrity, and that the signature will become unprotected if the record is changed (Dubai 2002, art. 20(1)). These guidelines emanated from the United Nations' "UNCITRAL" Model Law on Electronic Commerce (Blythe #1 2005). In the absence of contrary evidence, it is presumed that a "Protected" Electronic Signature is: (1) reliable; (2) is the signature of the person it purports to be; and (3) was used by that person to show agreement with the electronic record it is affixed to (Dubai 2002, art. 12(3)).

Reliance on a Protected Electronic Signature is presumed to be reasonable (Dubai 2002, art. 20(2)).

If the parties have agreed as to the application of prescribed or commercially reasonable authentication procedures to ensure that an electronic record has not been modified after a certain date, then the record is considered to be a Protected Electronic Record from that date forward (Dubai 2002, art. 19(1)). Factors to be considered in determination of whether the authentication methods are "commercially reasonable" include: (1) the type of transaction; (2) degree of knowledge and experience of the parties; (3) whether the parties often engage in similar transactions; (4) whether alternative procedures are readily available, and their cost; and (5) procedures generally used for similar transactions (Dubai 2002, art. 19(2)). In the absence of contrary evidence, it is presumed that a "Protected" Electronic Record: (1) was made by the party who purportedly made it; and (2) has not been altered since its creation (Dubai 2002, art. 12(4)).

Rules Pertaining to E-Commerce Agreements

Contract Formation

In the absence of a contrary agreement between the parties, a contractual offer and acceptance may be in electronic form (Dubai 2002, art. 13(1)). A contract shall not be denied legal effect merely because it was consummated using electronic communications (Dubai 2002, art. 13(2)).

Attribution

An electronic record may be assumed to have been sent from a particular sender if: (1) the record was sent as a result of the sender's acts (Dubai 2002, art. 15(1)); (2) the record was sent as a result of the sender's agent's acts (Dubai 2002, art. 15(2)(a)); or (3) the record was automatically transmitted by the sender's computer system (Dubai 2002, art. 15(2)(b)).

If the receiver does not have definite knowledge as to who sent a communiqué, the receiver is entitled to assume that the sender-in-question was the actual transmitter if: (1) the receiver applied a verification procedure previously agreed to by the sender (Dubai 2002, art. 15(3)(a)); or (2) the communiqué was received as a result of the actions of a person having a relationship with the sender (or his agent) so that the person was able to retrieve the message after becoming aware of a method used by the sender to identify her messages (Dubai 2002, art. 15(3)(b)).

If the receiver knows that a message was actually sent by the sender, or is entitled to so assume, then the sender may also assume that the message is what the sender intended to send, and act accordingly (Dubai 2002, art. 15(5)). If the receiver either knew or should have known that an error was made in the transmission, the receiver may not make this assumption (Dubai 2002, art. 15(7)).

Each message transmitted from the sender to the receiver may be interpreted by the receiver as a separate and independent communiqué. However, this interpretation is inapplicable if a reasonable person should have concluded that a second message was a duplicate of the first (Dubai 2002, art. 15(6)).

Notwithstanding the above: the receiver is not entitled to assume that a purported sender sent a communiqué if: (1) the purported sender has informed the receiver that he did not send the message; (2) the receiver either knew, or should have known, that the message did not originate with the purported sender; and (3) it would be unreasonable for the sender to assume that the purported sender actually sent the message, or to act on that assumption (Dubai 2002, art. 15(4)).

Acknowledgement of Receipt

The following rules do not cover the legal consequences which may result from an electronic communiqué or the acknowledgement of its receipt (Dubai 2002, art. 16(7)). These rules are applicable if either: (1) the sender (referred to in the ETL as the "originator") has requested the receiver (referred to in the ETL as the "addressee") to acknowledge receipt of the

message; or (2) the parties have agreed that an acknowledgement is to be sent from the receiver to the sender (Dubai 2002, art. 16(1)).

1. If the parties have not agreed as to the form or the method of the acknowledgement, then the acknowledgement may be given by: (a) any form of communication of the addressee, including automated communication; or (b) any conduct of the receiver that is “reasonably sufficient” to indicate reception (Dubai 2002, art. 16(2)).
2. If the sender states that the electronic message requires an acknowledgement, then the message is assumed never to have been sent until the sender receives the acknowledgement (Dubai 2002, art. 16(3)).
3. If the sender has not stated the message is conditional until receipt of acknowledgement, and no acknowledgement has been received by sender within the specified time or the time agreed to (or, if no time had been specified or agreed), then after a “reasonable time,” the sender: (a) may inform the receiver that no acknowledgement has been received, and may specify a reasonable future time certain for its receipt; and (b) if the acknowledgement referred to in (a) is not timely received, then the sender, after notice to the receiver, may act as though the message had never been sent, or pursue any other rights she may have (Dubai 2002, art. 16(4)).
4. When the sender receives an acknowledgement from the receiver, the sender may assume that the message has been received, but this assumption does not also necessarily mean that the message received is identical to the one that was sent (Dubai 2002, art. 16(5)).

If the acknowledgement states that “technical requirements” (either agreed to by the parties, or expressed in accepted standards) have been complied with, then it is presumed that those requirements have been met (Dubai 2002, art. 16(6)).

Assumed Time and Place of Sending and Receiving

Unless the sender and the receiver have agreed to the contrary, an electronic message is assumed to have been sent when it enters a computer system not under the control of the sender (Dubai 2002, art. 17(1)(a)).

Unless the sender and the receiver have agreed otherwise, the time of receipt is ascertained using the following rules. If the receiver has pinpointed a specific computer system the message should be sent to, receipt is assumed to occur when it enters that specific computer system; or, if the message is sent to one of the computer systems under the receiver’s control, but it is not the specific one that was requested, then receipt is assumed to occur when the receiver retrieves the communiqué; or, if the receiver has not designated

a computer system for the message to be sent to, receipt is assumed to have occurred when it enters a computer system belonging to the receiver (Dubai 2002, art. 17(1)(b)). These rules apply regardless of whether the location of the Information System is different from the location at which the electronic message is deemed to be received under ETL art. 17(3)—the place of business (Dubai 2002, art. 17(2)).

Unless the parties have a contrary agreement, then the message is assumed to have been sent from the sender's place of business, and received at the receiver's place of business (Dubai 2002, art. 17(3)). If either the sender or the receiver has more than one place of business, then the assumed point of transmission/reception is the one having the closest association with the transaction in question. If there is not a close association present, then the principal place of business is the applicable location (Dubai 2002, art. 17(4)(a)). If the party has no place of business, the point of transmission/reception is the residence of the party (Dubai 2002, art. 17(4)(b)). In the case of a corporation, the "usual place of residence" is the jurisdiction in which it is incorporated or the location of its main office (Dubai 2002, art. 17(4)(c)).

Certification Authorities

The issuers of Certificates are referred to as Certification Authorities ("CA") in this article because that is a more generally accepted international term. Instead of CA, Dubai law uses the term "Supplier of Certification Services" and defines it as follows: "Any confirmed or authorized person or entity that carries out the issuing of Electronic Authentication Certificates or any other services or tasks relating to them and to Electronic Signatures, as regulated under Chapter V of this law" (Dubai 2002, art. 2).

Appointment of Controller of Certification Services

The Chairman appoints the Controller of Certification Services ("Controller") to oversee and regulate the licensing and operational activities of Certification Authorities ("CA"). The appointment is to be made by an order published in the Official Gazette (Dubai 2002, art. 23(1)). The Controller is authorized to delegate her duties to subordinates (Dubai 2002, art. 23(2)). The Controller and her subordinates are considered to be "public servants," i.e., government employees (Dubai 2002, art. 23(3)). If a subordinate is in the process of exercising enforcement power against a third party, the subordinate must show proof of her authority to the third party if requested to do so (Dubai 2002, art. 23(4)).

Regulation of CA's

Regulatory rules pertaining to CA's are to be determined by the Controller, with approval required by the Chairman (Dubai 2002, art. 25). Those rules must cover: (1) licensing and renewal of licenses; (2) advertising and other activities of CA's; (3) business standards expected to be adhered to by CA's; (4) expected qualifications, experience and training of CA's and their employees; (5) conditions for the conduct of a CA's business; (6) documents to be distributed concerning a Certificate or a digital key; (7) the form and content of a Certificate or a digital key; (8) accounting practices; (9) expected qualifications of an auditor of the accounts of a CA; (10) inspection and control of CA's; (11) expected standards of any computer information system to be used by a CA; (12) conflict-of-interest rules pertaining to the relationship between a CA and its subscribers, and duties toward subscribers in reference to the Certificate; (13) licensing fees and other fees; and (14) forms to be used by CA's (Dubai 2002, art. 25(1)-(14)).

Duties of CA's

Certification authorities are mandated to do the following: (1) comply with any representations concerning its practices which have been made to its subscribers or other relevant parties; (2) use reasonable care to ensure that all information in the Certificate is accurate and that the information is complete; (3) provide relying third parties accessible information on the CA's website in reference to: CA identity, proof the subscriber had control of the private key, the means of identification of the subscriber, any limitations on purpose or value, whether the public key is valid and uncompromised, whether the signatory is able to give notice pursuant to ETL art. 22, (1)-(a), (b), and whether a timely revocation is available; (4) provide the subscriber with a method to give notice that the private key has been compromised, and promptly revoke the Certificate when this occurs; (5) employ a trustworthy computer information system, procedures and personnel; and (6) if a domestic CA, hold a license issued by the Controller (Dubai 2002, art. 24(1)).

These are factors to be considered in assessment of the trustworthiness of a CA's computer system, procedures and personnel: (1) financial and other assets in the firm; (2) reliability of hardware and software used in the computer information system; (3) procedures used in processing of applications for Certificates, issuance of Certificates, and retention of records; (4) making information regarding subscribers and CA services available to present or potential relying third parties; (5) frequency and intensity of independent audits of the CA; (6) declarations of the government, an independent accrediting organization or the CA itself that

the CA is in compliance with the above factors; (7) whether the CA is subject to the jurisdiction of the courts of the Emirate of Dubai; and (8) whether there is a divergence between the law pertaining to CA's and other law within the Emirate of Dubai (Dubai 2002, art. 24(2)).

Dubai has a compulsory licensing system for CA's; no CA may conduct business without a license. Another example of a country with a compulsory system is China. In some jurisdictions, however, the licensing is voluntary, with CA's free to conduct certification business even if they do not have a license. Examples are Hong Kong and Korea (see Blythe 2005 #4 and Blythe 2006 #5).

Required Contents of a Certificate

The formal term under Dubai law for a Certificate is "Electronic Authentication Certificate" An Electronic Authentication Certificate is defined as "A Certificate issued by a supplier of certification services providing in it an assurance as to the identity of the person or the party in control of a specific Signature Device, and which may be refereed (sic) to in this Law as the 'Certificate.'" The subscriber that is issued a Certificate by a CA is referred in the ETL as the Signatory. A signatory is defined as "A natural or legal person, holding his own Electronic Signature Device, and who signs or a signature is made on his behalf on an Electronic Communication by using such device (Dubai 2002, art. 2).

Upon receipt of an application for a Certificate, the CA will ask for identification documentation to be presented by the applicant. If satisfied that the applicant's purported identity is correct, and if all other information is presented and the fee is paid, the CA will issue the Certificate. The Certificate must contain the following information: (1) the CA's identity; (2) the subscriber's identity; (3) verification that the subscriber controlled the private key at the date of issuance of the Certificate; (4) verification that the private key was operational on or before the date the Certificate became effective; (5) any limitations on the purpose or value to which the Certificate may be used; and (6) any explicit limitations on the CA's liability toward any relevant person (Dubai 2002, art. 24(3)).

Liability of CA's

The general rule is that the CA is liable for any damages incurred by subscribers or relying third parties due to a defective or inaccurate Certificate. However, the CA's liability may be limited: (1) by any express limitations on scope and extent of liability expressed by the CA in the Certificate; or (2) if the CA is able to prove that it was not negligent or was

not at fault, or is able to prove that exogenous forces over which the CA had no control caused the damages, with the burden of proof upon the CA. (Dubai 2002, art. 24(4) and (5)).

Liability of Subscribers

When the subscriber electronically signs an electronic message, he does so using his private key. In the ETL, the private key is listed as one example of a Signature Device. A Signature Device is defined as “A device or Electronic Information prepared to operate independently or in conjunction with other devices and Electronic Information Systems to create a unique Electronic Signature attributable to a specific person; such an operation shall include any systems or devices which generate or capture unique information such as codes, algorithms, letters, numbers, private keys, personal identification numbers, (PINS), or personal attributes” (Dubai 2002, art.2). This definition is further evidence of the technological open-mindedness of the Dubai law. The ETL is written in a flexible manner and is not tied to any particular form of technology. Instead, it realizes that technology is continually evolving and that it would be unwise to choose one particular form of technology that would have the effect of exclusion of other forms. Nevertheless, the ETL grants most-favored-status to PKI.

A relevant factor in determination of a CA’s liability is whether the subscriber violated his duties. The subscriber is obligated: (1) to employ reasonable care over the private key and not allow it to be used in an unauthorized manner; (2) to promptly inform the CA and relying third parties whenever the security of the private key has been compromised, and whenever there is a substantial likelihood the security may have been compromised; and (3) to employ reasonable care to ensure that all material representations made to the CA when applying for issuance of the Certificate, and all information contained in the Certificate, are accurate (Dubai 2002, art. 22(1)). If the subscriber does not comply with his duties, he shall be responsible for any damages incurred by relying third parties (Dubai 2002, art. 22(2)).

Recognition of Foreign CA’s

Realizing that E-commerce is an international phenomenon, as a general rule the Emirate of Dubai grants reciprocal recognition to foreign CA’s, foreign-issued Certificates, and foreign-issued Electronic Signatures. The general rule has qualifications, however: (1) in the case of foreign-issued Certificates, the foreign CA’s practices in reference to issuance of Certificates must have a reliability level equivalent to or higher than that of those of CA’s in Dubai; and (2) in the case of Electronic Signatures, the laws

of the other jurisdiction must require a level of reliability at least as stringent as that of Dubai. In deciding whether the Certificate or the Electronic Signature is effective, any relevant agreement between the parties should be taken into account (Dubai 2002, art. 26(1), (2), (3) and (5)).

The parties may make an agreement as to: (1) a particular CA to be used; (2) a particular category of CA's to be used; or (3) a particular class of Certificates to be used. If the parties have agreed to use a particular type of Certificate or a particular type of Electronic Signature, that agreement is enforceable in the Emirate of Dubai (so long as the agreement is not in contravention of any other law of Dubai), notwithstanding the fact that the Certificate or the Electronic Signature was issued by a foreign CA. (Dubai 2002, art. 26(6)).

Computer Crimes

Fraudulent Publication of a Certificate

It is a crime to publish a Certificate with the name of a CA listed in it if the publisher knows that: (1) the CA named in the Certificate did not issue it; (2) the subscriber whose name is listed in the Certificate never accepted the Certificate; or (3) the Certificate has been suspended or revoked, unless the publication occurred prior to the suspension or revocation (Dubai 2002, art. 28). It is also a crime to knowingly create a fraudulent Certificate or provide false statements to a party for the purpose of acquiring a fraudulent Certificate. Convicted offenders shall be punished by imprisonment, a fine not to exceed 250,000 UAE Dirhams, or both (Dubai 2002, art. 29). [Two hundred fifty thousand UAE Dirhams is approx. U.S. \$ 68,064 as of 1 February 2006.]

Giving False or Unauthorized Information to a CA

Without prejudice to a more severe penalty provided in ETL art. 29 or any other law, it is a crime to knowingly provide untruthful information to a CA concerning one's identity or agency relationship for the purpose of achieving the issuance, suspension or revocation of a Certificate. Convicted offenders shall be punished by up to six months' imprisonment, a fine up to 100,000 UAE Dirhams, or both (Dubai 2002, art. 30). [One hundred thousand UAE Dirhams is approx. U.S. \$ 27, 225 as of 1 February 2006.]

Breach of Duty of Confidentiality

Any person who has obtained private information pursuant to the powers of the ETL has a duty to hold it in confidence; examples of such persons with confidential information include CA's and relevant government

officials. It is a crime to intentionally breach that duty by disclosing the information to a third party without permission. Convicted offenders shall be punished by imprisonment, a fine not to exceed 100,000 UAE Dirhams, or both. However, there are exceptions: (1) it is acceptable to disclose the information if the ETL requires it; (2) the information is needed in a court proceeding; or (3) disclosure is mandated because of a court order. (Dubai 2002, art. 31(1) and (2)).

Use of Electronic Means to Effectuate a Crime

The use of electronic means to carry out a crime is a separate criminal offense. Convicted offenders are subject to a maximum jail term of six months, a fine up to 100,000 UAE Dirhams, or both. If the punishment for the underlying crime is greater than this punishment, then the punishment for the underlying crime shall be applied (Dubai 2002, art. 32).

Corporate Offenders

If any part of the ETL or its implementation regulations are violated by a corporation, both the corporation as an entity and its individual managers and employees who were directly involved in (or who condoned) the unlawful acts will be charged with the offense and punished accordingly (Dubai 2002, art. 33).

Confiscation of Tools

The tools used by a convicted offender in the furtherance of computer crimes shall be confiscated by the court (Dubai 2002, art. 34).

Conciliation

In the case of first-time offenders, conciliation of the criminal case at any time is a possibility. If a conciliation settlement is reached before conviction, the criminal prosecution will be terminated. If a conciliation settlement is reached after conviction, the court's ruling will be suspended (Dubai 2002, art. 35).

Summary and Recommendations

Summary

Dubai's Electronic Transactions Law ("ETL") is designed to stimulate E-commerce in the emirate by improving the authenticity and integrity of electronic transactions. The ETL recognizes the legal validity of electronic documents and electronic signatures as acceptable substitutes for paper documents and ink signatures, respectively. Accordingly, electronic records may be used to comply with a statutory writing requirement, original

document requirement and retention requirement, and an electronic signature attached to an electronic document may be used to comply with a statutory requirement for a paper-and-ink signature. If all parties are in agreement, an E-commerce contract may be in electronic form. If a sender of an electronic message demands an acknowledgement of receipt, the message is not considered to have been received until the sender obtains the acknowledgement. Detailed contractual rules pertaining to attribution of electronic messages, and time/place of sending/receiving electronic messages, have been developed.

The ETL does not allow the use of electronic documents and electronic signatures in all situations, however. Paper documents and ink signatures are still required to be used for: wills, marriage certificates, divorce decrees, real property deeds, contracts pertaining to purchase or sale of real property, contracts to lease real property for more than ten years, negotiable instruments, and any document required to be notarized. Furthermore, the ETL does not mandate Dubai's government agencies to either accept or to utilize electronic documents. However, if they elect to do so, government agencies of Dubai may: allow electronic documents to be used by citizens in order to comply with a filing or retention requirement; issue licenses or permits in electronic form; accept or make payments or issue receipts using electronic means; issue public notices in electronic form; and use electronic means to ask for submission of bids and to issue acceptances to the successful bidders.

An unusual characteristic of Dubai's ETL is that the Chairman of the Dubai Technology, E-Commerce and Media Free Zone Authority ("Chairman") is given a great deal of discretionary authority and power in reference to the statute. For example, the Chairman: drafts and disseminates implementation regulations; appoints the Controller of Certification Services ("Controller") to license and regulate Certification Authorities ("CA"); has unilateral discretion to exempt any person or organization from the purview of the ETL; may establish special courts or tribunals to deal with E-commerce disputes; and has the discretion to determine whether a particular type of case is subject to the ETL.

In order to achieve more reliability and integrity in the utilization of electronic signatures in E-commerce, the ETL has created a compulsory system of licensing of CA's which is implemented by the Controller. The CA's role is to ascertain the identity of a subscriber and to attest in an issued Certificate that the electronic signature used by that subscriber belongs to him. The prospective CA must possess a high degree of expertise in reference to electronic signatures and computer information systems. If at

any time the Controller believes that a CA is no longer qualified to carry out its duties, the Controller may suspend or revoke the CA's license. Because E-commerce is an international phenomenon, the ETL provides for reciprocal recognition of CA's with licenses issued by foreign nations that have licensing standards that are at least as stringent as those of Dubai; the ETL also provides for reciprocal recognition of Certificates and Electronic Signatures that have been issued by foreign CA's. The CA may incur legal liability to its subscribers and to relying third parties if any information contained in the certificate is inaccurate. However, the CA's liability may be limited if the CA: has listed limitations on scope and extent of liability in the certificate; is able to prove that it was not negligent or not at fault; or is able to prove that external forces were the cause of the damages and the CA had no control over them. Furthermore, the subscriber (not the CA) is liable for damages to relying third parties whenever the subscriber: fails to maintain the security of the private key; does not give prompt notice to the CA whenever the security of the private key is jeopardized; and gives inaccurate information to the CA when applying for a Certificate.

The ETL contains a list of computer crimes. All of them are punished with fines, imprisonment, or both. It is a crime for a person or entity to: fraudulently publish a Certificate (the most stringently punished computer crime); give false or unauthorized information to a CA; breach a duty of confidentiality; or use electronic apparatus in order to carry out another crime. If a corporation is charged with a computer crime, the corporate managers and employees who participated in the crime will also be charged and held individually accountable. Any tools used in the commission of a computer crime will be confiscated by the government. However, if the party committing the crime is a first-time offender, there is a possibility that prosecution and trial can be avoided and that the matter can be settled through conciliation.

Recommendations

Dubai's ETL establishes a good basic framework for the attainment of secure E-commerce transactions. However, the following amendments are recommended for improvement of Dubai's E-commerce law.

Eliminate the Exclusion for Wills

The ETL excludes wills from its coverage. The result is that a will is required to be in paper form with a handwritten signature affixed to it in order to be enforceable. This exclusion should be eliminated. There is evidence that the aversion to electronic wills is beginning to dissipate. In 2005, the U.S. State of Tennessee became the first American jurisdiction to

recognize the legal validity of a will that is executed with an electronic signature (See Ross 2005).

Assert Long-Arm Jurisdiction against Foreign Parties

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

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 Blythe #6 2005).

More Consumer Protections for Participants in E-commerce

Dubai needs to enact a general consumer protection statute applicable to all internet consumers. The Republic of Tunisia can be used as a model for good consumer protections. The Tunisian E-commerce statute gives consumers: (1) a “last chance” to review an order before it is entered into; (2) a 10-day window of opportunity to withdraw from an agreement after it has been made; (3) a right to a refund if the goods are late or if they do not conform to specifications; and (4) no risk during the 10-day trial period after goods have been received. Tunisian E-consumers enjoy some of the best protections in the world (Tunisia 2000).

One of the few nations that may offer better consumer protections than Tunisia is the Republic of South Korea. That country has enacted a separate statute specifically for E-commerce consumer protections—the E-Commerce Transactions Consumer Protection Act (South Korea 2002). Iran also provides good consumer protections, including a window of opportunity to withdraw from an E-commerce transaction previously entered into; however, the window in Iran is only seven days, as opposed to Tunisia’s ten days (Blythe #7 2006).

New Computer Crimes

The list of computer crimes should be enlarged to explicitly prohibit computer hacking and to protect against computer tampering. The Computer Misuse Act of Singapore can be used as a model (Singapore #2 1993).

Information Technology Courts

Because of the specialized knowledge often required in the adjudication of E-commerce disputes, Information Technology Courts should be established as a court-of-first-instance for them. The I.T. Courts would be tribunals consisting of three experts. The chairperson would be an attorney versed in E-commerce law, and the other two persons would be an I.T. expert and a business management expert. The attorney would be required to hold a law degree and be a member of the bar with relevant legal experience; the I.T. person would be required to hold a graduate degree in an I.T.-related field and have experience in that field; and the business management expert would be required to hold a graduate degree in business administration and have managerial experience. The E-commerce law of the Kingdom of Nepal can be used as a model (Nepal 2005).

Mandatory E-Government

Mandatory (not merely permissive) requirements for governmental agencies to accept and issue electronic documents would expand E-government, resulting in more convenience for citizens, greater efficiency, and less cost. The E-Government Act of Finland can be used as a model (Finland 2003).

References

- ABA (American Bar Association), Section of Science & Technology, Information, Security Committee, Electronic Commerce & Information Technology Division, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce (ABA Net, 1995 and 1996) p. 9;
<http://www.abanet.org/ftp/pub/scitech/ds-ms.doc> .
- ABA (American Bar Association), PKI Assessment Guidelines, V 0.30 at 301 (Public Draft for Comment No. 25, 2001), p. 305;
<http://www.abanet.org/scitech/ec/isc/pagv30.pdf> .
- Abu-Ghazaleh Intellectual Property, AGIP Bulletin, 27 June 2005;
http://www.agip.com/bulletin_news.aspx?id=960&month=6&year=2005&lan...(Accessed 3 November 2005).
- Berman, Andrew B., Note, "International Divergence: The 'Keys' To Signing on the Digital Line—The Cross-Border Recognition of Electronic Contracts and Digital Signatures," 28 Syracuse Journal of International Law and Commerce 125, 143-44 (2001).
- Blythe, Stephen E. (#1), "Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security," 11:2 Richmond Journal of Law and Technology 6 (2005).
- Blythe, Stephen E. (#2), "Pakistan Goes Digital: the Electronic Transactions Ordinance as a Facilitator of Growth for E-commerce," 2:2 Journal of Islamic State Practices in International Law __ (2006).
- Blythe, Stephen E. (#3), "The Azerbaijan E-Commerce Statutes: Contributing to Economic Growth and Globalization in the Caucasus Region," 12 Columbia Journal of East European Law ____ (2006).
- Blythe, Stephen E. (#4), "Electronic Signature Law and Certification Authority Regulations of Hong Kong: Promoting E-Commerce in the World's 'Most Wired' City," 7 North Carolina Journal of Law and Technology 1 (2005);
- Blythe, Stephen E. (#5), "The Tiger on the Peninsula is Digitized: Korean E-Commerce Law as a Driving Force in the World's Most Computer-Savvy Nation," 28: 3 Houston Journal of International Law 573 (2006).
- Blythe, Stephen E. (#6), "South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga," 10: 1 Journal of South Pacific Law ____ (2006).
- Blythe, Stephen E. (#7), "Tehran Begins to Digitize: Iran's E-Commerce Law as a Hopeful Bridge to the World," 18 Sri Lanka Journal of International Law____ (2006).

- Blythe, Stephen E. (#8), "Singapore Computer Law: An International Trend-Setter with a Moderate Degree of Technological Neutrality," 33 Ohio Northern University Law Review ___ (2006).
- Chung, Rina C.Y., "Hong Kong's 'Smart' Identity Card: Data Privacy Issues and Implications for a Post-September 11th America," 4 Asian-Pacific Law and Policy Journal 442 (2003).
- CIA, U.S. Central Intelligence Agency, The World Factbook, "United Arab Emirates," (Last Updated 10 January 2006); <http://www.cia.gov/cia/publications/factbook/geos/ae/htm> (Accessed 1 February 2006).
- CPILive.Net, Dubai Internet City Visions, "Dubai Internet City—The Vision Continues,"p. 1; http://www.cpilive.net/news_ver2/guides_2005/dic_visions/dic_vision (Accessed 3 November 2005).
- Dessent, Michael, "Browse-Wraps, Click-Wraps and Cyberlaw: Our Shrinking (Wrap) World," 25 Thomas Jefferson Law Review 1, 4 (Fall, 2002).
- Dubai, Emirate of, Law of Electronic Transactions and Commerce No. 2/2002; http://www.tecom.ae/law/law_2.htm (Accessed 3 November 2005).
- EU Directive, European Union Directive 1999/93/EC of the European Parliament and of the Council of 13 DECEMBER 1999 on a Community Framework for Electronic Signatures, (1999/93/EC)—19 January 2000, OJ L OJ No L 13 p.12.
- Finland, Republic of, Act on Electronic Services and Communication in the Public Sector (13/2003), 2003; <http://www.finlex.fi> (Accessed 15 March 2006).
- Fischer, Susanna Frederick, "California Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation," Association of American Law Schools 2001 Annual Meeting, Section on Law and Computers, 7 Boston University Journal of Science and Technology Law 229, 233-237 (Summer, 2001).
- Froomkin, A. Michael, "The Essential Role of Trusted Third Parties in Electronic Commerce," 75 Oregon Law Review 49, 58 (1996).
- GCC. The formal name of this organization is the Cooperation Council for the Arab States of the Gulf; website is located at http://www.gcc-sg.org/home_e.html.
- Hallerman, David, "Will Banks Become E-commerce Authorities?," 12 Bank Technology News, June 1, 1999.

- Hogan, Tara C., Notes and Comments—Technology, “Now That the Floodgates Have Been Opened, Why Haven’t Banks Rushed Into the Certification Authority Business?,” 4 North Carolina Banking Institute 417, 424-27 (2000).
- ITP Technology (Information and Technology Publishing Co.), “Etisalat, FGB in e-commerce conference,” 26 October 2005; <http://www.itp.net/news/print.php?id=18561&prodid=&category=> (Accessed 3 November 2005).
- Khaleej Times, “E-Commerce Law Promulgated,” 16 February 2002; <http://www.khaleejtimes.co.ae/ktarchive/160202/lead.htm> (Accessed 3 November 2005).
- Mathia, Shilpa, Middle East Intelligence Bulletin, “E-initiatives in the GCC Region,” (December, 2000), p. 2, available at http://www.meib.org/articles/0012_me2.htm (Accessed 3 November 2005).
- Nepal, Kingdom of, Electronic Transactions Ordinance of the Year 2061 B.S. (2005 A.D.), ss 60-71. An official English version was released by the Nepal Ministry of Law, Justice and Parliamentary Affairs and was published in the Nepal Gazette on 18 March 2005; <http://www.hlcit.gov.np/pdf/englishcyberlaw.pdf> (Accessed 23 November 2005).
- Poggi, Christopher T., “Electronic Commerce Legislation: An Analysis of European and American Approaches to Contract Formation,” 41 Virginia Journal of International Law 224, 243, 249-51 (2000).
- Pun, K.H., Lucas Hui, K.P. Chow, W.W. Tsang, C.F. Chong & H.W. Chan, “Review of the Electronic Transactions Ordinance: Can the Personal Identification Number Replace the Digital Signature?,” 32 Hong Kong Law Journal 241, 256, 257 (2002).
- Qudah, S.M., “Legal Insight on the Dubai Electronic Transactions and Commerce Law No. 2 of 2002,” 17:3 Arab Law Quarterly 283-86.
- Roland, Sarah E., Note, “The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?” 35 Suffolk University Law Review 625, 638-45 (2001).
- Ross, Chad Michael, Comment, “Probate—Taylor v. Holt—The Tennessee Court of Appeals Allows a Computer Generated Signature to Validate a Testamentary Will,” 35 University of Memphis Law Review 603 (2005).
- Singapore, Republic of (#1), Electronic Transactions Act (Cap. 88), 10 July 1998; <http://agcvldb4.agc.gov.sg/> (Accessed 15 February 2006).

- Singapore, Republic of (#2), Computer Misuse Act (Cap. 50A), 30 August 1993;
http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_gettopo.pl?actno=1998-REVED-50A (Accessed 22 December 2005).
- Smedinghoff, Thomas J., "Electronic Contracts: An Overview of Law and Legislation," 564 PLI/P at 125, 146, 149, 162 (1999).
- South Korea, Republic of, Korean Legislation Research Institute, Act on the Consumer Protection in the Electronic Commerce Transactions ("CPA"), Statutes of the Republic of Korea, Vol. 13, pp. 481 to 485-30.
- Stern, Jonathan E., Note, "Federal Legislation: The Electronic Signatures in Global and National Commerce Act," 16 Berkeley Technology Law Journal 391, 395 (2001).
- Tang, David K.Y., "Electronic Commerce: American and International Proposals for Legal Structures," in Regulation and Deregulation: Policy and Practice in the Utilities and Financial Services Industries 333 (Christopher McCrudden ed., 1999).
- Tunisia, Republic of, Electronic Exchanges and Electronic Commerce Law, 2000; <http://www.bakernet.com.org> (Accessed 15 February 2006).
- UCA (Utah Code Annotated) 46-3-101 et seq. (1999).
- UCC (U.S. Uniform Commercial Code) ss 2-201 and 2-209 (1998).
- UN (United Nations), United Nations Commission on International Trade Law ("UNCITRAL"), Model Law on Electronic Commerce With Guide to Enactment, G.A. Res. 51/162, U.N. GAOR, 51st Sess., Supp. No. 49, at 336, U.N. Doc. A/51/49 (1996);
<http://www.uncitral.org/english/texts/electcom/ml-ecom.htm>
(Accessed 25 October 2005).
- USTR (Office of the United States Trade Representative), Reports: United Arab Emirates (2005);
http://www.ustr.gov/assets/Document_Library/Reports_Publications/2005/2005_NTE_Report/asset_upload_file865_7523.pdf (Accessed 10 January 2006).
- Wright, Benjamin, "Symposium: Cyber Rights, Protection, and Markets: Article, 'Eggs in Baskets: Distributing the Risks of Electronic Signatures,'" 32 West Los Angeles Law Review 215, 225-26 (2001).
- Zaremba, Jochen, "International Electronic Transaction Contracts Between U.S. and E.U. Companies and Customers," 18 Connecticut Journal of International Law 479, 512 (2003).
- Zhang, Chu and Lei Lingfei, "The Chinese Approach to Electronic Transactions Legislation," 9 Computer Law Review and Technology Journal 333, 343-46 (2005).

تشريع دبي للمعاملات الالكترونية: نموذج أولي لقانون التجارة الالكترونية في الإمارات العربية المتحدة ودول مجلس التعاون الخليجي

د. ستيفن بلايث
جامعة هونج كونج

ملخص

يهدف قانون دبي للمعاملات الالكترونية إلى تحفيز التجارة الالكترونية في الإمارة عن طريق تحسين صحة وسلامة المعاملات الالكترونية، حيث يعترف القانون بالصلاحيات القانونية للمستندات الالكترونية والتوقيعات الالكترونية كبدايل مقبولة للوثائق الورقية والتوقيعات بالحبر، فإذا اتفقت جميع الأطراف يجوز أن يكون العقد في شكل الكتروني وله نفس قوة التنفيذ القانونية للعقود المكتوبة على الورق. ولا يلزم التشريع الوكالات الحكومية بإمارة دبي باستخدام الوثائق الالكترونية، ولكنها قد تختار أن تفعل ذلك. وقد أوجد التشريع نظاماً إلزامياً لترخيص سلطات التصديق، ليكون دورها هو التأكد من هوية طالب الخدمة وإصدار شهادة بأن التوقيع الالكتروني الذي يستخدمه ينتمي إليه (يخصه). ويتضمن التشريع قائمة بالجرائم الحاسوبية، ويحدد إطاراً سليماً للتجارة الالكترونية، ولكن يمكن تحسينه بإضافة حماية للمستهلك، وزيادة قائمة الجرائم الحاسوبية، وإنشاء محاكم خاصة بهذه الجرائم تكون ذات نراع طويلة الاختصاص، وجعل الحكومة الالكترونية إلزامية، كما ينبغي إلغاء الاستثناء الخاص بالوصايا.