INTERNATIONAL HARMONIZATION IN ELECTRONIC COMMERCE AND ELECTRONIC DATA INTERCHANGE: A PROPOSED FIRST STEP TOWARD SIGNING ON THE DIGITAL DOTTED LINE*

RANDY V. SABETT**

TABLE OF CONTENTS

[*] Portions of this Essay first appeared in *The Electronic Banking Law & Commerce Report* ("EBLCR"), Vol. 1, No. 4, Sept. 1996. The EBLCR is available from Glasser LegalWorks, 150 Clove Road, Little Falls, N.J., 07424. To contact the publisher, send e-mail to legalwks@aol.com.

[**] Mr. Sabett is an Associate in the General Litigation Practice Group at Venable, Baetjer, Howard & Civiletti, L.L.P., in Washington, D.C. He is active in Venable's electronic banking practice and has more than five years of engineering experience in the government and commercial information security marketplace. Mr. Sabett joined Venable after serving as Smart Card Program Manager and Field Application Engineer at SPYRUS, Inc. He has extensive experience in the development of high grade cryptographic products to ensure confidentiality, authentication, and access control utilizing public/private key exchange methods. In addition, he is active in several organizations, including the Information Security Committee of the Section of Science and Technology of the American Bar Association. Within that committee he has served on the Editorial Committee for the Digital Signature Guidelines, and he is the co-chair of the Key Escrow Working Group that is focusing on the numerous issues involved in the commercial key escrow area.

Prior to joining Venable, Mr. Sabett also worked for the Department of Defense (National Security Agency) in the fields of software cryptography and embedded cryptographic modules. Mr. Sabett holds a Bachelor of Science degree in Computer Engineering from Syracuse University and a Juris Doctor degree from the University of Baltimore.

PREFACE

Scene: Board room of CyberConglomerate, a large Japanese technology firm.

Time: Late evening.

Setting: On one side of the table sit the directors of CyberConglomerate. On the other side, sits the CEO of a small California start-up company with his two VPs (i.e., the whole company). Discussions have been proceeding toward a deal whereby CyberConglomerate will license the start-up company's new software package.

Dialogue:

CYBERCONGLOMERATE PRESIDENT: We are pleased with the progress shown to date on the latest release of the software. We look forward to a beta test version once we have signed the documents.

START-UP COMPANY CEO: According to the documents we have drawn up, we will complete the modifications by the end of this quarter and begin shipping to you by the beginning of next quarter.

CYBERCONGLOMERATE PRESIDENT: Excellent. In light of that, the only thing left is to sign the contract. I will now sign.

[He uses his smart card[1] *to apply his digital signature to the documents and then passes them to the start-up CEO. A few seconds pass while the documents travel across the Internet.]*

START-UP COMPANY CEO: Received. I will sign also.
[He brings up his digital signature software on his palmtop, inserts his smart card, logs in using his biometric fingerprint reader, and also digitally signs the document.]

CYBERCONGLOMERATE PRESIDENT: That is all for now. Speak with you soon.

START-UP COMPANY CEO: Good day.

Epilogue: The two parties both reset their teleconference video walls, and in the Japanese office the directors go home for the evening. In the U.S. office, the start-up company goes to work.

This story depicts much more science than fiction. The technological capability that exists today would make this type of transaction a reality. The legal effect of such a transaction, however, would be dubious at best.

INTRODUCTION

For more than a decade, the legal community has sought to address the ubiquitous subjects of electronic commerce ("EC") and electronic data interchange ("EDI") at the international level.[2] During this time, the growth of open communications systems and EC has exploded.[3] Consequently, the gap between the outer reaches of law

[1] *See* Linda Kay Sakelaris, *Manufacturers Report Standards Will Drive Smart Card Market*, RADIO COMM. REP., Sept. 16, 1996, at 50, *available in* LEXIS, News Library, Curnws File (stating that smart card looks like credit card except that instead of having a magnetic strip encoded with the credit card number, a smart card contains a small electronic chip that can hold information).

[2] *See* G.A. Res. 40/71, U.N. GAOR, 40th Sess., 112th plen. mtg. at 2, U.N. Doc. A/RES/40/71 (1986) (calling "upon Governments and international organizations to take action . . . so as to ensure legal security in the context of the widest possible use of automated data processing in international trade" (citing *Report of the U.N. Commission on International Trade Law*, 18th Sess., Supp. No. 17, at 70-72, U.N. Doc. A/40/17 (1985))).

[3] Estimates vary widely on the size of the Internet, the primary forum for electronic commerce. One recent assessment stated that the Internet is doubling in size every three months. *See* Jack Egan, *Ready, Set, Search: Powerful Search Engines Dig Out What You Seek*, U.S. NEWS & WORLD REP., Apr. 29, 1996, at 64. Another study, conducted by Nielsen Media Research, indicated that the total number of Internet users ranges anywhere from 16 million

and the needs of the commercial community have widened. The law's ability to respond to changes in technology, most notably the Internet, remains in doubt. For a number of reasons, several of which this Essay will explore, progress has been slow in the alignment of international law with technology.

Part I of this Essay assesses recent activity and advances in public key cryptography and one potential application to international EC and EDI. Part I then examines the revolution in information security created by an area of mathematics known as public key cryptography and provides a short primer on cryptography leading into a discussion of digital signatures. Part II discusses the general areas of EC and EDI. Part III examines the existing systems of international business transactions, focusing particularly on the challenges that must be addressed to facilitate electronic transactions. In Part IV, a review of recent efforts provides insight into what should occur next. Finally, Part V suggests the specific mechanism of digital signatures as a catalyst for stimulating harmonization in international EC and EDI.

I. SECURITY SERVICES, PUBLIC KEY CRYPTOGRAPHY, AND DIGITAL SIGNATURES

An overview of the fundamental services provided by an information security system serves as the best introduction to public key cryptography in general and digital signatures in particular.[4] By focusing first on these essential services, a more thorough understanding of the interface between the security concepts involving cryptography and the underlying legal framework will result.

to 20 million. *See* Peter H. Lewis, *In a Recount, Cyber Census Still Confounds*, N.Y. TIMES, Apr. 17, 1996, at D1. Size notwithstanding, a recent study estimated that approximately $189 billion of business in goods and services will be transacted by the year 2000. *See* Jonathan Gaw, *Expectations Lowered for Internet Commerce*, STAR TRIB., May 1, 1996, at 1D.

[4] "Cryptography" is the use of codes, ciphers, algorithms, and other devices that scramble the content of electronically-sent messages so that only certain people can interpret and view the message. *See* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 713 (1995).

"Public key cryptography" is a practice begun in 1974 in which users employ two keys, one public and one private. *See id.* at 890. Messages encrypted with one key can be decrypted only with the other. *See id.* at 891. A "key" is a value used to encrypt messages by use of algorithms. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 3 (2d ed. 1996).

"Digital signatures" allow for authentification of messages by identifying the sender and connecting the sender to the message. *See* Froomkin, *supra*, at 895. If the message attached to the digital signature is altered in any way, the signature will not decrypt the message properly. *See id.*

In the situations described below, the author of a message (who is also described as the sender) composes the message[5] and transmits it to the receiver. In practice, this transmission likely would occur over an open communications system in which security and legal concerns would be significant.[6] The threat posed by unauthorized messages exists whenever a message travels over an information system accessible to outsiders.[7] Any such message can be vulnerable to misuse, unauthorized intervention, and manipulation.[8] Thus, for both legal and technical reasons, the sender would apply various mechanisms prior to sending the message to implement the following security services.

A. *Security Services*

The first security service, known as confidentiality,[9] assures both sender and receiver that the message could not have been understood by any unauthorized parties. If an eavesdropper were able to intercept the message, confidentiality theoretically renders it impossible for the interloper to interpret the message properly. The information security mechanism of encryption commonly provides this service.[10] Encryption mathematically scrambles the communication so that only the sender and recipient can unscramble and understand the original message.[11] It is important to note that the service of confidentiality is not provided via digital signature mechanisms.[12]

The second security service, known as integrity, assures the recipient that the message from the sender arrived intact. Unlike confidentiali-

[5] Note that the term "message" applies to any type of communication between two parties, whether text-based or otherwise. For example, a schematic of a printed circuit board being transmitted by a sender to a recipient would constitute a message.

[6] *See* Froomkin, *supra* note 4, at 720 (describing ease with which electronic mail can be forged and noting vulnerability of banks to electronic theft of funds).

[7] *See id.* at 722-25 (noting, for example, that as use of mobile communications such as cellular phones and inadequately protected computer networks increase, so do chances for exposure to high- and low-tech industrial espionage).

[8] *See* Raymond T. Nimmer & Patricia Krauthouse, *Electronic Commerce: New Paradigms in Information Law,* 31 IDAHO L. REV. 937, 945 (1995).

[9] Another common term for confidentiality is privacy.

[10] Encryption, the application of cryptography, is the process of disguising a message so as to hide its substance. *See* SCHNEIER, *supra* note 4, at 1.

[11] More accurately, the only people who can interpret and understand the original message properly are those in possession of the key to the algorithm used to encrypt the message. *See* Froomkin, *supra* note 4, at 886.

[12] *See* SCHNEIER, *supra* note 4, at 37 (explaining that digital signature algorithms do not encrypt). Although digital signatures will assure the recipient that the message received actually was sent by the named sender, they cannot guard against others viewing the message. *See id.* at 41 (citing, as example, use of digital signatures with seismic data exchanged between United States and Soviet Union to assure each nation that other is not tampering with outgoing data).

ty, this service does not thwart eavesdroppers.[13] An eavesdropper still could alter a message transmitted with only an integrity mechanism. The integrity mechanism, however, will alert the recipient of such an alteration.[14] Numerous methods exist that provide integrity, including checksums, hash functions, and error-correcting codes.[15] Unbeknownst to most individuals, each of these integrity mechanisms likely affects their daily routine by providing improved communications.[16]

The third security service, known as authentication, assures the recipient that only the sender could have created the message.[17] In many respects, authentication is the most easily understood of the security services described here. The concept of authentication fits well with the existing paradigm of a paper-based signature.[18] It assures the recipient of the authenticity of the sender's message.[19]

From a legal perspective, authentication is perhaps the most important of all of the security services. The ability to prove one's identity over vast distances, and to do so without ever having met the other party, significantly increases the viability of widespread international EC and EDI.[20] No longer are face-to-face meetings required for the signing of documents.[21] Although the ceremonial

[13] Eavesdroppers commonly are referred to as adversaries, attackers, interceptors, interlopers, intruders, opponents, or "the enemy." *See id.* at 4.

[14] *See* Committee on Payment and Settlement Systems & the Group of Computer Experts of the Central Banks of the Group of Ten Countries, *Security of Electronic Money*, at 29, Annex 1, Glossary (Aug. 1996) (visited Jan. 8, 1997) <http://www.systemics.com/docs/papers/BIS_smart_security.html> (on file with *The American University Law Review*) (defining integrity as "the quality of being protected against accidental or fraudulent alteration or of indicating whether or not alteration has occurred").

[15] *See* SCHNEIER, *supra* note 4, at 30 (describing hash function as "a function, mathematical or otherwise, that takes a variable-length input string . . . and converts it to a fixed-length (generally smaller) output string"). Hash functions and other integrity mechanisms are useful for "fingerprinting" files to allow for easy verification. *See id.* at 31.

[16] For example, data transmission equipment such as modems and fax machines employ integrity mechanisms to detect and correct errors. *See* FRED HALSALL, DATA COMMUNICATIONS, COMPUTER NETWORKS AND OPEN SYSTEMS 125-37 (4th ed. 1996) (providing detailed discussion of error detection methods, including parity, checksums, and cyclic redundancy checks).

[17] *See* SCHNEIER, *supra* note 4, at 52 (explaining that authentication device allows recipient to verify that sender is not impersonating someone else). For example, the use of a password prior to conducting electronic banking at an automated teller machine is a process of authentication. *See id.*

[18] *See id.* at 35-36. The paradigm holds that paper-based signatures are valuable because the signature is unforgeable, authentic, not reusable, unalterable, and cannot be repudiated. *See id.*

[19] *See* Froomkin, *supra* note 4, at 895 ("If the cipher is strong and the key tightly guarded, the use of the correct cipher strongly suggests that the message was sent by the person it purports to be from.").

[20] *See id.* at 895 n.798 (noting that digital signatures in conjunction with private keys can be used to authenticate electronic messages and sender's identity).

[21] *See id.* at 895 & n.798; SCHNEIER, *supra* note 4, at 38-39 (describing use of digital signatures and public key cryptography to sign legal documents).

aspect of "signing" a document will continue to exist, the method by which this function occurs will shift from paper to electronic.

Nonrepudiation, the fourth security service, although technologically similar to authentication, provides a different type of security. It assures the recipient that the author of a message cannot, at a later time, deny having transmitted the message to the recipient.[22] The concept of nonrepudiation, which has evolved from the information security field, can cause confusion because there is no such thing in the legal vernacular as nonrepudiation. Further adding to the confusion is the contract law concept of repudiation.[23] Repudiation occurs when one party reverses its earlier affirmative decision to enter into a contract. That is, the party repudiates the contract. Because a party always can try to breach a contract, there really is no legal notion of nonrepudiation. In information security, however, the concept of nonrepudiation is well established.

B. What Is Public Key Cryptography?

Cryptographic discussions extensively use the word "key."[24] The term evolved from the analogy of a physical key used to lock and unlock something. In cryptography, the key metaphor relates to the locking and unlocking of data. A cryptographic key enables a user to transform data according to some prescribed algorithm.[25] The key itself has no recognizable form; it is simply a particular arrangement of information to be used by a cryptographic algorithm. A key, when represented as readable characters, might look something like this:

h7$*R1nJ&85#{3Bw .

Two more common terms are "encryption" and "decryption," which apply to the processes of scrambling and unscrambling data using a cryptographic key and a prescribed algorithm. The encryption process renders the original data, or "plain text,"[26] unreadable,

[22] *See* Charles R. Merrill, *An Attorney's Roadmap to the Digital Signature Guidelines*, *in* Doing Business on the Internet 379, 383 (PLI Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series No. 64-3988, 1996).

[23] *See* John D. Calamari & Jospeh M. Perillo, The Law of Contracts § 12-4 (3d ed. 1987) (defining repudiation as: (1) positive statement indicating promisor cannot or will not perform; (2) transfer to third party of interest in anything essential for performance; or (3) voluntary affirmative act rendering performance impossible).

[24] *See supra* note 4 (explaining use of electronic key in cryptography).

[25] In modern cryptography, only the key, and not the algorithm itself, must be concealed to protect the security of the message. *See* Froomkin, *supra* note 4, at 886. Encryptions using multiple keys usually need only keep one key secret. *See id.* at 886 n.768.

[26] "Plain text" refers to data that has not been "locked" or encrypted by the cryptographic key. Plain text, for example, might be a document or an e-mail message in readable form.

whereas the decryption process (the reverse of the encryption process) manipulates the "cipher text"[27] to restore the original data.

Public key cryptography[28] owes its existence to a branch of mathematics known as computational number theory[29] and involves various techniques such as modular reduction,[30] discrete logarithms,[31] factoring of large prime numbers, and, most importantly, one-way functions. A one-way function furnishes security by providing a relatively easy computation in one direction, but an extremely difficult computing problem when the original computation is reversed.[32] Effectively, it is impossible to reverse the first computation with the computing power available today. A detailed discussion of these concepts goes beyond the scope of this Essay, but several good references exist.[33]

Prior to the introduction of public key cryptography in the 1970s,[34] encryption technology was highly specialized.[35] In contrast to public key techniques, the earlier systems used an approach known as secret key cryptography.[36] This approach (still in use today) requires that all users have the identical key in order to communicate

[27] "Cipher text" refers to information that has undergone the cryptographic transformation that "locks" the data. Once plain text has been converted to cipher text, it is no longer readable.

[28] *See supra* note 4 (defining public key cryptography). Typically, encryption is done by the public key, and decryption is performed by the private key. *See* SCHNEIER, *supra* note 4, at 39. Almost anyone, therefore, can encrypt a message, but only those with access to the private key can decrypt it. *Id.*

[29] *See* SCHNEIER, *supra* note 4, at 198 (detailing computational number theory).

[30] *See id.* at 242.

[31] *See id.* at 261-63 (discussing significance of discrete logarithms in finite group to cryptography).

[32] This is referred to as a trap-door, one-way function. *See id.* at 30. An effective metaphor for understanding this phenomenon is the process of taking a watch apart and then attempting to reassemble it: disassembling the watch is simple, but putting it back together is extremely difficult without instructions. *See id.*

[33] *See generally id.* (providing thorough overview of entire field of cryptography, from high-level conceptual information to low-level coding). For a detailed and highly-theoretical discussion of the underlying mathematical concepts on which public key cryptography is based, see 2 DONALD E. KNUTH, THE ART OF COMPUTER PROGRAMMING, SEMINUMERICAL ALGORITHMS (2d ed. 1981). Other excellent sources of information about these concepts include Froomkin, *supra* note 4; and Visa, *Tomorrow: Electronic Commerce* (visited Sept. 18, 1996) <http://www.visa.com/cgi-bin/vee/sf/standard.html> (on file with *The American University Law Review*) (discussing Secured Electronic Transaction ("SET") standard adopted to safeguard credit card purchases made over open networks).

[34] *See generally* Whitfield Diffie & Martin Hellman, *New Directions in Cryptography*, 22 IEEE TRANSACTIONS ON INFORMATION 6 (1976); R. Rivest et al., *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, 21 COMMUNICATIONS OF THE ACM 120 (1978).

[35] "Highly specialized," in this context, means the lack of widespread use of the technology, coupled with the lack of interoperable systems and protocols. Early cryptographic systems usually were unique for each application, both in terms of physical implementation and the algorithms utilized.

[36] *See* Froomkin, *supra* note 4, at 890 (discussing disadvantages to secret key cryptography).

securely. Implementation of such a system involves distributing those keys to all parties and updating the keys on a frequent basis. At least two drawbacks exist in a secret key system. First, compromise of the secret key by one user compromises the entire communications network for all users.[37] Second, numerous opportunities exist for a compromise to occur in a secret key system.[38] Because the secret key must be handled by more than one person in a key distribution system, the danger exists that compromise could occur at any point.

Unlike secret key cryptography, public key cryptography involves a system of mathematically related information known as a public/private key pair. The key pair enables a user to publicly distribute a piece of information (the public key), which then can be used by others to communicate securely with that user.[39] The user retains the private key, preferably in a hardware token. This approach alleviates the need for all users in a system to have the same secret key in advance. Instead, each user simply posts his or her public key where other users can access it.[40]

The cryptographic basis of a public key cryptosystem addresses both drawbacks cited above that exist in secret key cryptosystems. First, because each user has a different public/private key pair, a compromise would not affect the entire system. Also, most competent implementations of public key cryptography never allow the secret key to leave the cryptographic token.[41] Further, the secret key usually is well protected.[42] Thus, the likelihood of a disclosure of the private key is minimized.

C. *What Is a Digital Signature?*

The concepts underlying public key cryptography manifest themselves in digital signatures as well as in encryption and

[37] *See id.*

[38] *See id.*

[39] *See* SCHNEIER, *supra* note 4, at 31-32; Froomkin, *supra* note 4, at 891.

[40] The posting of a public key is somewhat analogous to publishing a phone number in the telephone book. In the not-so-distant future, the process of looking up someone's e-mail address in a public directory of information will become a common occurrence. From this directory, the person's certificate could be retrieved, enabling the retrieving party to communicate securely with the person whose identity is bound to that public key. The Consultative Committee on International Telephone and Telegraph ("CCITT") has recommended one such system, known as X.500.

[41] A "cryptographic token" is a broad term for the physical medium that carries the cryptographic key. For example, two of the most common and most promising personal cryptographic tokens are the PCMCIA card and the smart card.

[42] *See* SCHNEIER, *supra* note 4, at 32 (observing that private key cannot be deduced from public key).

decryption.[43] The structure of a public/private key pair also exists in a digital signature scheme.[44] Whereas encryption uses the public key to encrypt and the private key to decrypt the data, however, a digital signature scheme based on public key cryptographic techniques utilizes the private key to sign the message.[45] Correspondingly, the public key verifies the digital signature.[46] Thus, in an encryption scheme, anyone can secure data that is to be sent to the recipient, but only the recipient can decrypt because only the recipient possesses the secret key. Similarly, in a digital signature scheme, only the signer can produce the digital signature because only the signer has the secret key. Because the public key is publicly available, however, anyone having access to that public key can verify the signature.[47]

Several publications discuss digital signatures, but few provide an example. What follows is a sample message with a cryptographically-based digital signature attached:

—BEGIN SIGNED MESSAGE—

ACME DIGITAL PRODUCTS, INC.
Purchase order number: 4789
Date: Dec. 21, 1996

This message represents a valid purchase order for: 1000 widgets at the quoted price of: $100/each from vendor: VENDOR ONE
Terms: Net 30

—END SIGNED MESSAGE—
Public Key ID # F3CA9C473B06
Public Key available at:
http://www.not_a_real_url.com/username/publickey.html

—BEGIN SIGNATURE—

Version: 2.6.2
Comment: VENDOR ONE Purchase Order

[43] *See id.* at 37-41 (discussing process of using public key algorithms for digital signatures and encryption).

[44] *See id.* at 39 (describing act of signing by use of digital signature algorithms as "encrypting with a private key" and verifying the signature as "decrypting with a public key").

[45] *See id.*

[46] *See id.*

[47] *See* Froomkin, *supra* note 4, at 895 n.798 (illustrating that anyone with sender's public key can decrypt digitally signed message and can be reasonably certain it was not sent under fraudulent circumstances because only sender, in possession of private key, could have encrypted the message).

```
iQCVAwUBAnqXtNMvW01AQFR4Jw21lp8bpe/uUbC3QcSn+HLP
UugQDCDpaS8HVk/RwiUWRDvy7gFD71yM48cKvgcSoV51zW3n5
jybEntN1gZYHVCtbjdJa30x4rRtO7nb
```

—END SIGNATURE—

Due to the mathematical basis of public key cryptography, a digital signature is simply a stream of digits that appears unintelligible to the human observer; however, it actually possesses a significant amount of information. In commercial implementations, the digital signature probably would not be displayed to the user. Instead, upon the successful verification of the signature, the communication mechanism would provide an indication that the verification of the digital signature was successful and display the identity of the signer. This information would be made available as a result of the certificate used to verify the signature.

A digital signature utilizes sophisticated and elegant mathematical techniques to provide security services that are critical to international EC and EDI. First, and most importantly for EC and EDI, a digital signature provides authentication. Authentication assures the recipient of a verified digital signature that only the sender could have created the message to which the digital signature was applied.[48] Authentication is analogous to a handwritten signature on a document, hence the "digital signature" appellation.[49] Due to the binding between each signed message and the signer, however, a digital signature actually provides even stronger authentication than a handwritten signature. Whereas a paper-based signature exists on and authenticates only the last page (or, at best, each page, if in fact each page is initialed), a digital signature effectively provides authentication of every bit that makes up every character within the message. One might view a digital signature as an application of one's initials to each and every letter that constitutes the message.[50] This means that unlike a handwritten signature, digital signatures differ for each and every message that a user sends.[51]

[48] *See id.* (discussing verification advantages in public key digital signatures).

[49] Handwritten signatures are, in theory, authentic, unforgeable, non-reusable, unalterable, and cannot be repudiated. *See* SCHNEIER, *supra* note 4, at 35. Digital signatures created by public-key algorithms provide the same characteristics as handwritten signatures. *See id.* at 37-38.

[50] *See* Froomkin, *supra* note 4, at 895 (noting that message that has been digitally signed by private key will not decrypt properly if it has been altered even slightly).

[51] *See id.* (explaining that message that has been digitally signed by private key will not decrypt properly if signature was forged by copying it from different message).

Next, a digital signature provides nonrepudiation. This assures the recipient of a message verified with a digital signature that the sender later cannot deny having sent the message. Were this to occur, the recipient could prove the authorship of the message by using the sender's public key in combination with the received message. In verifying the digital signature using the sender's public key, the recipient would have the proof that only the holder of the corresponding private key could have created the original message. Although closely related to the concept of authentication, nonrepudiation is conceptually distinguishable. Whereas authentication provides assurance only of the origin of the message, nonrepudiation assures that the sender of the message cannot deny sending the message.

Finally, most common digital signature algorithms provide integrity via a mechanism known as a hash function.[52] A hash function reduces a set of bits of arbitrary length to a fixed length known as a hash result (or simply a hash).[53] In doing so, a hash function must possess three important characteristics. First, it must be computationally infeasible to derive another meaningful message that would result in the same hash value.[54] This means that someone

[52] A hash function provides a means by which a message of arbitrary length can be reduced to a generally smaller, fixed-length value, and by which it can be consistently computed for a given set of information. As an example, a simple, non-cryptographic (and weak) hash function might involve simply adding the ordered values for each character in a message and ignoring any carries past two digits. Thus, 'A' or 'a' would have a value of 1, 'B' or 'b' would have a value of 2, etc. In this example, we might define a space as having a value of 27, a comma as having a value of 28, and a period as having a value of 29. Given the following message:

This is a sample message.

the hash value would be equal to 357. This was computed by adding up T=20, h=8, i=9, s=19, space=27, etc., for the entire message.

In order to provide integrity, the sender would calculate a hash value for a message, and would use that value to calculate the digital signature. The recipient would calculate a hash value for the received message and would use that hash value to verify the signature. Using the example above, if the message had been changed (either innocently or maliciously) to:

This is a simple message.

the hash value would be equal to 365. The mismatch in values, which would result in an error when trying to verify the digital signature, would be an indication that the integrity of the message had been compromised.

Note that the simplicity of this hash function (which actually is a simple checksum) is intended to illustrate how such a function works. In actual practice, this hash function would not be adequate because its simplicity would allow the relatively easy computation of a message with an identical hash value. Instead, secure hash functions are one-way cryptographic transformations that cannot be reversed. *See* SCHNEIER, *supra* note 4, at 30.

[53] The term "hash result" also commonly appears in information security literature as a "message digest." *See id.* at 353, 435-36 (explaining operation of message digest in detail).

[54] *See* DIGITAL SIGNATURE GUIDELINES, LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND ELECTRONIC COMMERCE 36 (Info. Sec. Comm., Elec. Com. & Info. Tech. Div., A.B.A. Sci. & Tech. Sec. 1996) [hereinafter DIGITAL SIGNATURE GUIDELINES].

cannot purposely create a message that makes sense and that also will yield a hash value identical to one for a different message that also makes sense.[55] Second, it must be computationally infeasible to derive the original message from the hash value.[56] This means that the message corresponding to a given hash value should not be determinable only by knowledge of the hash value. For example, given a hash value of hash1, the underlying message (msg1) could not be determined. Finally, the hash result should be identical for a given algorithm and a given input.[57] This means that regardless of the implementation, identical hash results will occur for a given message and algorithm. In other words, for a message (msg1), the chosen hash function will yield the same hash value (hash1) every time for that message.

D. How Digital Signatures Work

Handwritten signatures traditionally have served several legal purposes. For example, a written signature can be used as evidence,[58] as a ceremonial function, as a designation of approval,[59] and as a determination of authenticity.[60] A digital signature can fulfill all of these purposes without changing the existing paradigm of a person "signing" a document. The digital signature exchange involves two parties directly. At the sending end, the signer creates a message and then uses a cryptographic processing package to produce the digital signature.[61] The signer uses the private key of

[55] In mathematical terms, this would mean that the hash of a meaningful message (msg1), which yields a hash of hash1, could not also result when a second meaningful (but different) message (msg2) is hashed with the same algorithm. For example:
If:
$\mathrm{hash}(\mathrm{msg1}) = \mathrm{hash1}$
and
$\mathrm{hash}(\mathrm{msg2}) = \mathrm{hash2}$
then
$\mathrm{hash1} \neq \mathrm{hash2}$ when $\mathrm{msg1} \neq \mathrm{msg2}$
for a given hashing algorithm.

[56] *See* DIGITAL SIGNATURE GUIDELINES, *supra* note 54, at 36.

[57] *See id.*

[58] *See* Stanley A. Kurzban, *Authentication of Computer-generated Evidence in the United States Federal Courts*, 35 IDEA 437, 459 (1995) (arguing that rules for authenticating computer-generated signatures used as evidence are based on use of hand-written signatures as evidence).

[59] *See* DIGITAL SIGNATURE GUIDELINES, *supra* note 54, at 4.

[60] *See* Judith Y. Gliniecki & Ceda G. Ogada, *The Legal Acceptance of Electronic Documents, Writings, Signatures, and Notices in International Transportation Conventions: A Challenge in the Age of Global Electronic Commerce*, 13 NW. J. INT'L L. & BUS. 117, 134 (1992).

[61] A cryptographic processing package may be hardware-based, software-based, or some combination of the two. For example, a digital signature might be calculated using a software program running on a computer. The digital signature also might be calculated within a hardware token such as a smart card or PC card. There are advantages and disadvantages to both methods. The use of a hardware token provides the strongest security because the private

the public/private key pair to generate the digital signature on the message and then binds the digital signature to the message. At the receiving end, the recipient uses the signer's public key to verify the digital signature.

E. Public Key Infrastructure

For all of this sophisticated and elegant mathematical processing to be implemented properly, a segment of the informational infrastructure must serve to certify the validity of a particular holder of a public/private key.[62] The prevailing validation model consists of a hierarchy of entities, commonly known as certification authorities ("CA"), that provide a level of trust to a public key infrastructure.[63] A CA is a licensed third party[64] which validates the digital signatures of authors or other subscribers to its service.[65] One area of continuing legal evolution concerns the allocation of liability within this type of system.[66]

At the heart of a public key infrastructure is the notion of a certificate.[67] A certificate contains a user's name and public key.[68] Thus, a certificate links the identity of the holder of the private key to a corresponding public key. From a legal standpoint, the CA and the subscriber share in the liability associated with the digital signature mechanism.[69] By certifying the subscriber's certificate, the CA states that the subscriber has satisfied the requirements specified by the CA.[70]

key never leaves the confines of the token. Hardware tokens, however, tend to be slightly more expensive than a software package. In contrast, a software package might be somewhat less expensive but provides much less security because the private key resides in the untrusted host computer.

[62] *See* Henry H. Perritt, Jr., *Access to the National Information Infrastructure*, 30 WAKE FOREST L. REV. 51, 99-100 (1995).

[63] *See* SCHNEIER, *supra* note 4, at 186 (discussing role of certification authorities).

[64] It is expected that each state will license their CAs. *See infra* note 138.

[65] *See* SCHNEIER, *supra* note 4, at 186.

[66] *See generally* MICHAEL BAUM, NAT'L INST. OF STANDARDS & TECH. FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY: LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES (1994) (providing thorough treatment of issues involving certification authorities).

[67] *See* SCHNEIER, *supra* note 4, at 426; *see also* Charles R. Merrill, *What Lawyers Need to Know About the Internet*, *in* A CRYPTOGRAPHY PRIMER 187, 192 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course Handbook Order No. 443, 1996) (noting importance of certification authorities to public key cryptography system).

[68] *See* Merrill, *supra* note 67, at 193.

[69] *Cf. id.* at 194 (discussing electronic commerce model using single central figure to interact with many subscribers without certificate authority liability).

[70] For example, a CA with minimal certification requirements might require a subscriber to fill out a form. At another level, the CA might require the subscriber to fill out a form and provide proof of identity, perhaps via a driver's license or passport. For each possible scenario, the associated liabilities would be analogous to the requirements. In the first example above,

II. OPEN SYSTEMS, ELECTRONIC COMMERCE, AND ELECTRONIC DATA INTERCHANGE

The computer revolution of the 1980s forever altered the business landscape by changing the manner by which information is transmitted and consumed. It soon became apparent that the potential for this new technology would be limited only by the imagination of those with the vision to apply it to a myriad of life's situations. More importantly, it became evident that the repercussions of this information revolution would far exceed the effects of the transition from handwriting to mechanical printing.[71] The computer has become an electronic version of Gutenberg's printing press, with an even greater impact on society.

Although the expectations and realities of the Internet do not necessarily coincide, they continue to converge. Whether the Internet's global information infrastructure eventually will replace a majority of current business channels remains the topic of much debate.[72] Numerous obstacles exist, even when limiting the scope to a national view. At the international level, further impediments to the pervasive use of technology among nations persist. International EC and EDI can become a successful reality only when these obstacles have been addressed in such a way that businesses feel secure in employing the technology.

In order for this revolution to occur, a legal framework must be erected that will delineate the rights, responsibilities, and liabilities of

the CA might waive all liability with regard to the proper identity of the subscriber. In the second scenario, the CA might accept some limited liability for any problem associated with the identity of the subscriber.

[71] Some effects include:

(1) The ability to access instantly an enormous amount of information. Prior to the computer, one was limited by the physical availability of the desired written resources. Now, a single electronic connection can provide a great wealth of information.

(2) The ability to instantly process information. Prior to the computer, significant effort needed to be spent on relatively time-consuming and repetitive tasks. Now, electronic spreadsheets, databases, and word processors (to name just a few of the commercial applications) have made numerous tasks much easier and faster. Consequently, more time can be spent on more substantive work.

(3) The relative ease with which communications can occur among people in very diverse cultures.

[72] *See* Christine Curtis, *EDI over the Internet: Let the Games Begin*, COMM. WK., Sept. 9, 1996, at 59 (contending that more corporations will engage in electronic data interchange on Internet as costs decrease and security improves); Art Hutchinson, *Pushing the Envelope: Vendors Ready for War over Securing Content Control and Distribution*, COMM. WK., Sept. 2, 1996, at 508 (noting that developing software technologies will enable many business functions to take place on Internet). *But see* Jim Sabo, *Riding Shotgun on the Electronic Stagecoach*, NET GUIDE, Aug. 1, 1996, at 119 (warning that lack of security on the Internet may dissuade businesses from expanding into electronic commerce).

the various parties involved. International electronic transactions will not occur on a vast scale unless the law provides adequate clarity with respect to EC and EDI.

Numerous interpretations exist about the precise meaning of the commonly heard terms "electronic commerce" and "electronic data interchange." For example, one definition describes EDI as a "service by which corporations can send payments and invoices electronically to trading partners via banks."[73] Another definition focuses on the facilitation of exchanging electronic information via the combination of computers and telecommunications systems.[74] According to one definition, EC involves the electronic transfer of funds in commercial transactions.[75] For the purposes of this discussion, EC means any transaction involving an electronic analog for one of the traditionally "paper-based" elements of a commercial transaction.

III. BARRIERS TO INTERNATIONAL EC/EDI TRANSACTIONS

The growth of open electronic systems has matured to the point at which one naturally would expect international electronic transactions to be commonplace.[76] Based on other examples of modernization that have been adapted for use in international transactions, such as fax machines, the next logical progression would involve pervasive global electronic transactions.[77] However, several factors contribute to the relative rarity of international EC and EDI systems.[78] Barriers to this evolution must continue to be examined, and accommodations must be made so that the introduction of electronic business systems become the norm rather than the exception.

Existing business and legal infrastructures embrace a technology that had its beginnings more than 500 years ago. The reliance on paper-based systems presents a formidable barrier to the adoption of

[73] Brian O'Keefe, *Automated Clearing House Growth in an International Marketplace: The Increased Flexibility of Electronic Funds Transfer and Its Impact on the Minimum Contacts Test*, 15 U. PA. J. INT'L BUS. L. 105, 114 (1994).

[74] *See* Jeffrey B. Ritter, *Current Issues in Electronic Data Interchange: Defining International Electronic Commerce*, 13 NW. J. INT'L L. & BUS. 3, 17-20 (1992).

[75] *See* George A. Zaphiriou, *Unification and Harmonization of Law Relating to Global and Regional Trading*, 14 N. ILL. U. L. REV. 407, 413 (1994).

[76] *See* James Gleick, *Dead as a Dollar*, N.Y. TIMES, June 16, 1996, § 6 (Magazine), at 27-29 (describing decline of cash use and increase of electronic transfers of funds).

[77] *See id.* at 29-30 (discussing experiments by financial and telecommunication companies that envision global electronic transactions).

[78] *See* BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE: EDI, E-MAIL, AND INTERNET: TECHNOLOGY, PROOF, AND LIABILITY §§ 4.3, 7.3, 10.1, 13.4 (2d ed. 1995) (offering exhaustive treatment of existing barriers to electronic commerce including risks associated with novelty of field, unsettled law, and skeptical courts and range of problems from best evidence rule to Internet security).

electronic means of conducting business.[79] Nonetheless, once the international business community better understands the close analogies between traditional, paper-based security mechanisms and electronic technologies, it will embrace the technology.[80] The foothold of existing paper-based systems eventually will be replaced by globally accepted electronic means. To facilitate this transition, harmonization of both legal and technical perspectives must occur.

In many instances, domestic and international law formalities overtly or implicitly restrict business transactions to paper-based systems. The commercial world long has relied on paper documents.[81] As a result of this dependence, the paper requirement in commercial transactions significantly limits the acceleration of electronic commerce.[82] Further, formal requirements that differ among international parties could handicap EC and EDI to the point at which the technology offers little advantage over existing paper-based systems.[83] Requirements for documents, writings, and notice contribute to this particular barrier.[84]

Traditional letter of credit ("LOC") transactions exemplify the paper documentation paradigm in international transactions. These transactions consist of "the LOC itself, the draft, and all of the various shipping and insurance documents that frequently accompany the draft"[85] and traditionally have been "awash in paper documentation."[86] Manually processing this paperwork unnecessarily inflates the cost of these transactions. Accelerating the use of EC and EDI in this area would reduce significantly, and perhaps even eliminate, the associated costs.[87]

[79] *Cf.* Udo Flohr, *Electric Money*, BYTE, June 1996, at 74-76 (noting that consumers and merchants perceive bills and coins as having real value, unlike "electric money").

[80] *See id.* at 76 (describing efficiency rewards of having underlying financial networks that are "open, scalable, and able to interweave consumers with retailers, material suppliers, and financial institutions").

[81] *See* R. David Whitaker, *Letters of Credit and Electronic Commerce*, 31 IDAHO L. REV. 699, 700 (1995).

[82] *See* Jeffrey B. Ritter & Judith Y. Gliniecki, *International Electronic Commerce and Administrative Law: The Need for Harmonized National Reforms*, 6 HARV. J.L. & TECH. 263, 264 (1993) (describing how current legal structures in statutory and regulatory areas validate enforceability of commercial transactions via paper media).

[83] *See* Gliniecki & Ogada, *supra* note 60, at 132.

[84] *See id.*

[85] Whitaker, *supra* note 81, at 700.

[86] *Id.*

[87] *See id.* at 706-07 (introducing alternative to existing paper-based letter of credit practice). Professor Whitaker describes an automated letter of credit transaction. *See id.* Within this model, he alludes to the need for a low-level method of authentication. *See id.* A digital signature would be the ideal method to meet this need.

One well-known anecdote describes another situation in which significant cost savings could result from the use of EC and EDI. An average ship carries 500 pounds or more of paperwork related to the cargo on board.[88] All the information contained within those documents, if reduced to a common format, easily could be stored electronically. Electronic storage not only would free space and reduce weight, but it also would facilitate rapid transferal of the information once the goods were delivered.[89]

In addition to the limitations regarding legal requirements for paper documents, the requirements for a handwritten signature provide an even more significant limitation. The signature requirement "may be the single greatest obstacle to electronic commerce."[90] Although progress has been made in reducing the limitations of handwritten signature requirements in the four years since that statement was made, the handwritten signature remains a significant impediment.[91]

At a recent conference,[92] one presenter provided a poignant example of the commercial world's unwillingness to abandon the handwritten signature. CygnaCom Solutions, Inc., provides a paperless mortgage processing system to Chemical Bank.[93] The system provides a hierarchy of trust, via an issuer, custodian, and releaser.[94] Both the issuer and the custodian apply their respective digital signatures to the mortgage pool information.[95] The releaser verifies the two digital signatures and archives the transaction.[96] The irony within the system is the inclusion of a digitized signature[97] of both the issuer and the custodian. Thus, a system exists that embeds a handwritten signature within a packet of data that has a digital

[88] *See* Ritter, *supra* note 74, at 17.

[89] *See id.*

[90] Gliniecki & Ogada, *supra* note 60, at 134-35.

[91] *See, e.g.*, Ritter & Gliniecki, *supra* note 82, at 269 (noting that although commercial practice and rules develop around barriers of manual signatures, "only positive regulatory reform will transform these administrative requirements into a media-neutral environment that facilitates the evolution of electronic commerce").

[92] RSA Day in Washington, D.C., Apr. 25, 1996.

[93] *See* Santosh Chokhani, BSAFE and Banking Security (Apr. 25, 1995) (written materials distributed at RSA Day in Washington, D.C., on file with *The American University Law Review*).

[94] *See id.*

[95] *See id.*

[96] *See id.*

[97] The reader should be careful to note the difference between a "digitized signature" and a digital signature. A digitized signature is simply an electronic representation of a handwritten signature. The electronic form of a handwritten signature can be produced using a scanner or other electronic means. There is no cryptographic basis to this method, however, and the digitized signature offers none of the additional security services provided by the mathematics of a digital signature (e.g., data integrity, nonrepudiation, and authentication).

signature applied to it.[98] Although the use of digital signature technology in this system is laudable, the retention of the handwritten signature provides an ideal example of the adherence to prior formalities.

Another barrier involves the slow rate of reaction by the law to technological advances. In one particular domestic example, a task force working on Article 2 of the Uniform Commercial Code ("U.C.C.") commented that technological developments "not envisioned by the drafters of Article 2 . . . test the capacity of the Code to keep pace with business developments."[99] In contrast to the development of the law, the growth of technology continues to accelerate at an incredible pace.[100] Thus, the interpretation of existing law and the development of new law must occur in such a way that business is encouraged to rely on new technologies. When governmental regulation operates, the mandates should focus on functional areas instead of technical issues.[101]

IV. EFFORTS TO DATE

Some commentators suggest that harmonization between commercial practice and international law is necessary to facilitate the widespread acceptance of EC and EDI.[102] To determine a path forward, existing efforts first must be analyzed to identify barriers that have been overcome and those that remain.

The general areas where advances have occurred fall into the following two categories: transactional functions and notarial functions. Transactional functions involve those that occur between two parties in various types of business arrangements. Notarial functions involve attestation of documents and administration of oaths. The examples that follow illustrate where progress has been made in these two areas.

[98] *See* Chokhani, *supra* note 93.

[99] Roy R. Anderson et al., *An Appraisal of the March 1, 1990, Preliminary Report of the Uniform Commercial Code Article 2 Study Group*, 16 DEL. J. CORP. L. 981, 1038 (1991).

[100] One measure of such growth, known as Moore's Law, postulates that the number of transistors that can be placed on a single computer chip will double every two years. This theory has held true since Gordon Moore, one of the co-founders of Intel Corp., first predicted the trend more than 20 years ago. *See* Robert Lenzner, *The Reluctant Entrepreneur*, FORBES, Sept. 11, 1995, at 162.

[101] *See* Perritt, *supra* note 62, at 98.

[102] *See* Gliniecki & Ogada, *supra* note 60, at 118.

A. *Transactional Functions*

One type of transactional function on which progress has been made in the EDI area involves credit transfers. The United States already has enacted Article 4A of the U.C.C. to cover these transactions. Internationally, the United Nations Commission on International Trade Law ("UNCITRAL") has adopted a model law covering credit transfers.[103] According to UNCITRAL's web page:

> [The Model Law,] adopted in 1992, deals with operations beginning with an instruction by an originator to a bank to place at the disposal of a beneficiary a specified amount of money. It covers such matters as the obligations of a sender of the instruction and of a receiving bank, time of payment of a receiving bank and liability of a bank to its sender or to the originator when the transfer is delayed or other error occurs.[104]

This description, and the detail found in the language of the model law, clearly indicates the desire by UNCITRAL to provide guidance in the low-level, detailed areas of EC that businesses need to make their decisions. Unlike high-level harmonizing language, which merely reduces barriers but does not provide detailed solutions, model laws provide the necessary details to facilitate the acceptance of electronic transactions.

UNCITRAL also has made progress with regard to the international repercussions of EDI. It recently produced a Draft Model Law on Legal Aspects of Electronic Data Interchange and Related Means of Communication ("Model Law").[105] The Model Law "applies to any kind of information in the form of a data message used in the context of commercial activities."[106]

Another transactional area implicating international EC involves a system similar to the domestic Automated Clearing House ("ACH") mechanism. An ACH system electronically facilitates the process of clearing checks. Essentially, it is "the electronic equivalent [of] the paper check processing system."[107] Recognizing the utility of such a system, and the benefits that it would provide on an international scale, the European Commission has been examining the utility of a

[103] *See* UNCITRAL, *UNCITRAL Model Law on Int'l Credit Transfers International Trade* (visited Nov. 16, 1996) <http://ra.irv.uit.no/trade_law/financecredit-transfers/uncitral-ml/txt/ml-int-credit-trans.complete.html> (on file with *The American University Law Review*).

[104] *See id.*

[105] *Report of the U.N. Commission on International Trade Law*, U.N. GAOR, 50th Sess., Supp. No. 17, U.N. Doc. A/50/17 (1995).

[106] *Id.* at 41.

[107] O'Keefe, *supra* note 73, at 105.

super-ACH system.[108] Such a system, if it were to develop, would require a significant amount of international cooperation due to the differences in the banking systems of the various parties involved.[109] Once established, a super-ACH system would simplify international transactions.

The hindrances to internationalization of the system are readily discernible even with regard to extending the U.S. ACH system to include Canada. Although the technology might exist to complete ACH transactions between the two North American neighbors, problems such as float periods, standards, settlement, and risk management remain unresolved.[110] Nevertheless, the benefits that would accrue from such a system make investigation of the possible implementation of a U.S.-Canadian ACH system worthwhile.

In response to the absence of clear legal guidance regarding EC and EDI, the Electronic Messaging Services Task Force, under the auspices of the American Bar Association, began a study in 1987 to "examine the effects of electronic commerce upon fundamental principles of contract law and related legal issues."[111] As a result of the study, the group undertook further work that led to the development of a Model Electronic Data Interchange Trading Partner Agreement and Commentary ("Model TPA"), which contains provisions covering electronic exchange of transactional business information.[112] The Model TPA provides a framework by which EDI, "in substitution for conventional paper-based documents," can be used to facilitate transactions.[113]

Of particular note in the Model TPA is its treatment of signatures.[114] Although still requiring a signature, the Model TPA affords to the parties considerable flexibility in defining what will be acceptable.[115] It also specifically notes that existing technology, sophistication of the parties, and applicable standards must be taken into consideration when deciding which signature technology to use.[116]

One criticism of the Model TPA approach to facilitating EDI centers on its perceived limitations. The argument essentially claims that the endorsement by the business and legal communities of

[108] *See id.* at 106.

[109] *See id.* at 112-13.

[110] *See id.* at 114.

[111] Michael S. Baum et al., *Model Electronic Data Interchange Trading Partner Agreement and Commentary*, 45 BUS. LAW. 1645, 1718 (1990).

[112] *See id.* at 1719.

[113] *See id.* at 1721.

[114] *See id.* at 1731 (providing § 3.3 cmt. 2).

[115] *See id.*

[116] *See id.*

trading partner agreements as private rule-making processes imposes limitations that actually run counter to an open system EC/EDI.[117] Such private agreements, however, promote the growth of EC and EDI by fostering the use of electronic mechanisms.[118] Although the particular approach chosen by trading partners ultimately might prove to be different than the approach that the business world adopts as a standard, those entities who pioneer EC and EDI methodologies will excel.[119] Therefore, the use of TPAs should not be curtailed.

Other examples of progress in the transactional area include the following: (1) the adoption of the Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission ("UNCID") by the International Chamber of Commerce ("ICC") in 1987;[120] (2) the development by a United Nations working group of a standard format for international EDI messages known as the Electronic Data Interchange for Administration, Commerce, and Transport ("UN/EDIFACT");[121] and (3) the adoption by the European Community of the Trade Electronic Data Interchange Systems ("TEDIS") program.[122] In addition, one recent proposal would extend the use of EDI to fungible agricultural goods.[123]

B. *Notarial Functions*

Another significant international legal area affected by advances in technology consists of notarial functions. In the international context, the concept of a notary goes far beyond the American notion of a notary public. A notary in the United States refers to the common-law concept of a public officer authorized to administer oaths, take acknowledgment of deeds, and attest to the authenticity of a person's signature.[124] In contrast, a notary in most foreign jurisdictions refers to the civil-law concept of a legal professional who provides a corresponding higher level of authentication and certification in numerous transactions.[125] A civil-law notary, such as those

[117] *See* Ritter & Gliniecki, *supra* note 82, at 266.

[118] *See id.*

[119] *See id.* at 266-67.

[120] *Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission ("UNCID")*, International Chamber of Commerce, ICC Doc. 452 (1988).

[121] *See* Amelia H. Boss, *The International Commercial Use of Electronic Data Interchange and Electronic Communications Technologies*, 46 BUS. LAW. 1787, 1796 (1991).

[122] *See id.* at 1793.

[123] *See* Donald B. Pedersen, *Electronic Data Interchange as Documents of Title for Fungible Agricultural Commodities*, 31 IDAHO L. REV. 719, 720-21 (1995).

[124] *See* BLACK'S LAW DICTIONARY 1060 (6th ed. 1990).

[125] *See* Theodore S. Barassi, *The Cybernotary: Public Key Registration and Certification and Authentication of International Legal Transactions* (visited Sept. 23, 1996) <http://www.intermarket.com/ecl/cybrnote.html> (on file with *The American University Law*

in Europe and Latin America, undergo demanding training and testing in addition to being lawyers.[126]

The United States Council for International Business has advanced the notion of a "Cybernotary" to more closely align the United States with international notarial practice.[127] This group seeks to establish the Cybernotary as a recognized legal entity.[128] A Cybernotary would be a lawyer well versed in international business, EC, EDI, and information security.[129] In particular, lawyers in this capacity must be proficient in digital signature technology[130] because a significant portion of their duties will involve authentication of electronic documents.

V. A PROPOSED PATH FORWARD: INCREMENTAL TECHNICAL AND LEGAL HARMONIZATION BEGINNING WITH THE SPECIFIC AREA OF DIGITAL SIGNATURES

Notwithstanding the barriers to global electronic transactions, the foregoing examples of progress toward international harmonization in electronic transactions provide a good starting point. Existing legal barriers that inhibit or prevent electronic transactions gradually will be eliminated. Without further legal guidance regarding specific electronic mechanisms such as digital signatures, however, these efforts will be of limited value.

Each of the transactions described above would require some sort of authentication. A harmonized model law or set of guidelines on digital signatures would apply in all of the areas cited as examples. Thus, for technology to be used to its fullest potential, progress also must be made at the low levels, where the details of the law need further definition.[131] In particular, the low-level details of international EC and EDI must be clarified in order for electronic transactions to be implemented widely and used effectively.

A cryptographically strong—and industry and academically proven—method of authentication, digital signature technology should be afforded international legal recognition as a means for

Review).

[126] *See id.*

[127] *See* Kathleen Murphy, *Cyber-Certification* (visited Sept. 23, 1996) <http://www.webweek.com/96Feb/news/cybernotaries.html> (on file with *The American University Law Review*).

[128] *See id.*

[129] *See id.*

[130] *See* Victoria Slind-Flow, *Moving into Cyberspace as Notaries: Legal Locksmiths*, NAT'L L.J., Dec. 18, 1995, at A1.

[131] *See* Peter Seipel, *The Technology of Insight: Computers and Informed Citizens*, 69 CHI.-KENT L. REV. 417, 418 (1993).

satisfying existing signature requirements. To further this goal, a common set of rules or guidelines addressing digital signatures should be developed. An international set of rules would provide a strong legal and technical basis for further harmonization. International guidelines would allow lawmakers to understand better the interaction of the legal and technical aspects of this useful mechanism. Furthermore, such guidelines would be widely applicable because signature requirements will continue to exist.

The technology of digital signatures provides stronger assurances of security than those provided by handwritten signatures. Digital signatures not only assure the recipient that the sender actually sent the message, but they also ensure the integrity of the data and guarantee nonrepudiation.[132] As a result, a digital signature on an electronic document can serve as an ideal foundation on which to build an internationally harmonized EC and EDI framework.

A. *Technical and Legal Issues Must Be Addressed Together*

Global acceptance of digital transactions can be accomplished only through a combination of both technical and legal efforts. On the technical side, technologists must consider the international repercussions of the systems that they design and field. Keeping abreast of the international systems that exist and of those that are being designed, information security professionals must strive to develop systems that will transcend national boundaries and provide capabilities that will withstand the rigors of the law.

On the legal side, the introduction of internationally acceptable rules and guidelines provides an impetus for companies to use the technology. Without such legal guidance, the commercial community likely would be unwilling to embrace the technology. A parallel can be drawn to the rulemaking that occurred in the United States in response to the electronic trading of corporate securities.[133] Without rules to address this new activity, no means existed by which disputes could be resolved.[134] As a result, Article 8 of the U.C.C.

[132] *See supra* Part I.A (describing security services offered by digital signatures).

[133] *See* Ritter & Gliniecki, *supra* note 82, at 271 n.20 (citing Charles·W. Mooney, Jr., *Beyond Neutrality: A New Model for Transfer and Pledge of Interests in Securities Controlled by Intermediaries*, 12 CARDOZO L. REV. 305 (1990)). Professor Mooney examines the use of traditional property law constructs in resolving claims to fungible bulks of securities. Professor Mooney argues that a new model focusing on the relationship of the claimants to the intermediaries would better serve the purpose of the claims. *See id.* at 271.

[134] *See id.* at 271 n.20.

provides rules covering the transfer of legal rights without the exchange of paper stock certificates.[135]

B. *United States as Leader*

As a technology leader, the United States should take an active role in furthering international harmonization efforts involving technology. Several domestic efforts already underway could and should be adapted to an international setting. For example, the Information Security Committee of the Section of Science and Technology of the American Bar Association has produced a set of Digital Signature Guidelines.[136] These guidelines provide a technically and legally sound framework by which consistent legislation can be modeled, both domestically and internationally. Thus, the guidelines exemplify the type of model document that would serve well the objectives outlined above.

At the domestic level, several states either have enacted digital signature legislation or are considering bills.[137] Although those implementing legislation must avoid introducing new barriers,[138] the initiative of these progressive states to address this technology represents a major step forward in the proliferation of EC and EDI.

CONCLUSION

The international business world stands poised to embrace currently available EC and EDI technology in order to increase efficiency and to reduce cost. To facilitate the acceptance of these technologies,

[135] *See* U.C.C. § 8-102(6) (1996) ("'Communicate' means to: (i) send a signed writing; or (ii) transmit information by any mechanism agreed upon by the persons transmitting and receiving the information.").

[136] *See* DIGITAL SIGNATURE GUIDELINES, *supra* note 54.

[137] The following states have passed legislation regarding digital signatures or have such legislation pending: Arizona, ARIZ. REV. STAT. § 41-121 (1996); California, CAL. GOV'T CODE § 16.5 (West 1996); Florida, Electronic Signature Act of 1996, 1996 Fla. Laws ch. 224; Georgia, H.R. 1256, 143d Leg., 96th Reg. Sess. (Ga. 1996) (creating House Digital Signatures Study Committee to examine need for legislation addressing authentication of electronic messages); Hawaii, H.R. 3759, 18th Leg., Reg. Sess. (Haw. 1996) (introducing Hawaii Digital Signature Act); S. 2401, 18th Leg., Reg. Sess. (Haw. 1996) (establishing pilot program in which state agency acts as certification authority to verify digital signatures of attorneys, notaries, and other persons authorized to use such signatures on electronic documents); Illinois, H.R. 3394, 89th Leg., Reg. Sess. (Ill. 1996) (authorizing use of digital signatures with electronic communications between state agencies and comptroller); Utah, UTAH CODE ANN. § 46-3 (1996); Virginia, H.R. 822, Reg. Sess. (Va. 1996) (introducing Virginia Digital Signature Act); and Washington, Electronic Authentication Act, ch. 250, 1996 Wash. Laws 1190.

[138] For example, if a state were to introduce legislation with significant licensure requirements, it might present too formidable of an entry barrier to companies considering entering the business. Similarly, if a number of states implement legislation with significantly different licensure requirements, the difficulty of obtaining a license in all of these states might present another entry barrier.

international harmonization must occur at all levels. Existing high-level barriers must be eliminated, and corresponding detailed rulemaking must occur. Approaches at low levels with wide acceptance also should be sought to provide a solid foundation upon which further progress may be made.

One ideal candidate for progress at the low level involves digital signature technology based on public key cryptographic techniques. The widespread use of this technology in the area of international business will lead to more efficient and more cost-effective transactions. Because public key technology in general, and digital signature technology in particular, has matured significantly, now is an ideal time to elevate the technology to a level of legal acceptability, both domestically and internationally. With domestic efforts underway, international acceptance should be the next logical step.